

Contents

Sicherheit und Zuverlässigkeit

Ihre Reise in die Datenschutz-Grundverordnung (DSGVO) für Windows Server 2016

Einrichten des Host-Überwachungsdiensts (HGS) für eine geschützte Fabric und abgeschirmte VMs

Übersicht

Planen

Planen für Hoster

Kompatible Hardware

Planen für Mandanten

Bereitstellen

Schnellstart

Bereitstellen von HGS

Voraussetzungen

Anfordern von Zertifikaten

Installieren von HGS

Neue Gesamtstruktur (Standard)

Geschützte Gesamtstruktur

Initialisieren von HGS

TPM-Modus

Tastenmodus

AD-Modus

Konfigurieren von HTTPS

Hinzufügen von Knoten

Bereitstellen geschützter Hosts

Voraussetzungen

TPM-Modus

Tastenmodus

AD-Modus

Bestätigen des Nachweises

Verwenden von VMM

Bereitstellen von abgeschirmten VMs

- Erstellen eines Windows-Vorlagendatenträgers

- Erstellen eines Linux Vorlagendatenträgers

- Einrichten des Windows Azure Packs

- Erstellen einer Antwortdatei für die BS-Spezialisierung

- Erstellen einer geschützten Datendatei

- Bereitstellen einer abgeschirmten VM mithilfe von PowerShell

- Bereitstellung mit VMM

- Bereitstellung mit Windows Azure Pack

- Abschirmen einer vorhandenen VM

Verwalten

- Verwalten des Host-Überwachungsdiensts

- Überlegungen zu Filialen

- Upgrade eines überwachten Fabric auf Windows Server 2019

Problembehandlung

- Diagnosetool für geschützte Fabrics

- HGS

- Überwachte Hosts

- Abgeschirmte VMs

Integritätsnachweis für Geräte

- Deaktivieren von Systemdiensten in Windows Server 2016

- Deaktivieren von benutzerbezogenen Diensten in Windows

Windows-Authentifizierung

- Windows-Authentifizierung: Technische Übersicht

- Windows-Authentifizierungskonzepte

- Windows-Anmeldeszenarios

- Architektur der Windows-Authentifizierung

- Architektur der Security Support Provider-Schnittstelle

- Anmeldeinformationen-Prozesse in der Windows-Authentifizierung

- In der Windows-Authentifizierung verwendete Gruppenrichtlinieneinstellungen

- Schutz und Verwaltung von Anmeldeinformationen

Konfigurieren von zusätzlichem LSA-Schutz

Neuerungen beim Schutz von Anmeldeinformationen

Schützen abgeleiteter Domänenanmeldeinformationen mit Credential Guard

Schützen von Remotedesktop-Anmeldeinformationen mit Remote Credential Guard

Sicherheitsgruppe „Geschützte Benutzer“

Authentifizierungsrichtlinien und Authentifizierungsrichtliniensilos

Gruppenverwaltete Dienstkonten

Erste Schritte mit gruppenverwalteten Dienstkonten

Erstellen des KDS-Stammschlüssels der Schlüsselverteilungsdienste

Kerberos-Authentifizierung

Neuerungen bei der Kerberos-Authentifizierung

Public Key Authentication für Geräte in einer Domäne

Eingeschränkte Kerberos-Delegierung

Verhindern, dass ein Kennwort, das geheime RC4-Schlüssel verwendet, von Kerberos geändert wird

Konfigurieren von Kerberos für IP-Adressen

NTLM

Kennwörter

TLS - SSL (Schannel SSP)

TLS-Änderungen in Windows 10 und Windows Server 2016

Verwalten von TLS

TLS-Registrierungseinstellungen

Schannel Security Support Provider: Technische Referenz

TLS-Protokoll (Transport Layer Security)

Datagramm-TLS-Protokoll (Transport Layer Security)

Funktionsweise der Benutzerkontensteuerung

Tokenbindung

Windows Defender Antivirus

TIP

Suchen Sie nach Informationen zu älteren Versionen von Windows Server? Sehen Sie sich unsere [Windows Server-Bibliotheken](#) auf „docs.microsoft.com“ an. Sie können auch nach bestimmten Informationen [auf dieser Website](#) suchen.

Windows Server Security bietet in das Betriebssystem integrierte Schutzebenen, die Sie vor Sicherheitslücken schützen, böswillige Angriffe blockieren helfen und die Sicherheit Ihrer virtuellen Computer, Anwendungen und Daten verbessern.

Blogbeitrag zur Windows Server-Sicherheit

In diesem Blogbeitrag des Windows Server-Sicherheitsteams werden viele der Verbesserungen in Windows Server beschrieben, mit denen die Sicherheit beim Hosten und in Hybrid Cloud-Umgebungen erhöht wird.

Datacenter and Private Cloud Security Blog (Blog zur Sicherheit in Rechenzentren und Private Clouds)

Dies ist die zentrale Blogwebsite für technische Inhalte des Microsoft Datacenter and Private Cloud Security-Teams.

Addressing emerging threats and landscape shifts (Reaktion auf neue Bedrohungen und Änderungen der Systemlandschaft)

In diesem sechsminütigen Video vermittelt Anders Vinberg zunächst einen Überblick über die Sicherheits- und Zusicherungsstrategien von Microsoft und spricht über Branchentrends und sicherheitsrelevante Veränderungen in der Systemlandschaft.

Blogbeitrag „Protecting Your Datacenter and Cloud from Emerging Threats“ (Schützen von Rechenzentren und Cloudumgebungen gegen neue Bedrohungen)

In diesem Blogbeitrag wird erläutert, wie Sie Microsoft-Technologien einsetzen können, um Ihre Rechenzentrums- und Cloudinvestitionen gegen neue Bedrohungen zu schützen.

Ignite-Sitzung mit einer Übersicht über „Sicherheit und Zuverlässigkeit“

Inhalt dieser Ignite-Sitzung sind dauerhafte Bedrohungen, Sicherheitsverstöße durch interne Mitarbeiter einer Organisation, organisierte Internetkriminalität sowie das Absichern der Microsoft Cloud Platform (lokale und mit Azure verbundene Dienste). Dabei werden u. a. Szenarien für das Schützen von Workloads, großen Unternehmensmandanten und Diensteanbietern beschrieben.

Sichere Virtualisierung mit abgeschirmten VMs

Abgeschirmte VMs auf Channel 9

Exemplarische Vorgehensweise zu abgeschirmten VMs und Beschreibung der Vorteile

Video zu abgeschirmten VMs

In diesem 4-minütigen Video werden der Nutzen abgeschirmter VMs sowie die Unterschiede zwischen einer abgeschirmten VM und einer nicht abgeschirmten VM erläutert.

Video mit exemplarischer Vorgehensweise „Shielded Virtual Machines in Windows Server“

In diesem Video mit exemplarischer Vorgehensweise wird gezeigt, wie der Host-Überwachungsdienst die Verwendung abgeschirmter virtueller Computer ermöglicht, damit sensible Daten vor einem nicht autorisierten Zugriff durch Hyper-V-Hostadministratoren geschützt werden.

„Harden the Fabric: Protecting Tenant Secrets in Hyper-V“ (Absichern des Fabrics: Schützen geheimer Mandantendaten in Hyper-V) (Ignite-Video)

Diese Ignite-Präsentation erläutert Erweiterungen in Hyper-V, Virtual Machine Manager und eine neue Host-Überwachungsdienst-Serverrolle zur Aktivierung von abgeschirmten VMs.

Guarded Fabric Deployment Guide (Bereitstellungsleitfaden für geschütztes Fabric)

Dieser Leitfaden umfasst Installations- und Validierungsinformationen für Windows Server und System Center Virtual Machine Manager für Hosts mit geschütztem Fabric und abgeschirmten VMs.

Abgeschirmte VMs und geschützte Fabrics in Filialen

Dieses Handbuch enthält bewährte Methoden für die Ausführung von abgeschirmten virtuellen Computern in Filialen und anderen Remoteszenarien, in denen Hyper-V-Hosts Zeiträume mit eingeschränkter Konnektivität zu HGS haben können.

Shielded VM and Guarded Fabric Troubleshooting Guide (Leitfaden zur Problembehandlung für abgeschirmte VMs und geschütztes Fabric)

In diesem Leitfaden finden Sie Informationen zur Behandlung von Problemen, die in Ihrer Umgebung mit abgeschirmten VMs auftreten können.

Artikel zu abgeschirmten VMs

In diesem Whitepaper können Sie sich einen Überblick darüber verschaffen, wie sich die Sicherheit mit abgeschirmten VMs verbessern lässt und wie Sie Manipulationen mithilfe dieser VMs verhindern können.

Härtung des Betriebssystems und der Anwendungen

Bereitstellungshandbuch zu Windows Defender-Anwendungssteuerung (WDAC)

Bei der WDAC handelt es sich um eine konfigurierbare Richtlinie zur Codeintegrität (CI), die Unternehmen dabei hilft zu steuern, welche Anwendungen in ihrer Umgebung ausgeführt werden. Sie hat keine speziellen Hardware- oder Softwareanforderungen, muss jedoch unter Windows 10 ausgeführt werden.

Demovideo zu Device Guard

Device Guard ist eine Kombination aus WDAC und Hypervisor-geschützter Codeintegrität (HVCI). Dieses siebenminütige Video enthält Informationen über Device Guard und seine Verwendung unter Windows Server.

Registrierungseinstellungen für Transport Layer Security

Informationen zu unterstützten Registrierungseinstellungen für die Implementierung des Transport Layer Security (TLS)- und des Secure Sockets Layer (SSL)-Protokolls unter Windows.

Ablaufsteuerungsschutz

Der Ablaufsteuerungsschutz bietet integrierten Schutz gegen einige Fälle von Speicherbeschädigungsangriffen.

Windows Defender

Windows Defender bietet Funktionen zum aktiven Schutz, um bekannte Schadsoftware zu blockieren. Windows Defender ist standardmäßig aktiviert und für die Unterstützung der verschiedenen Serverrollen in Windows Server optimiert.

Privileged Access Management (Schützen von Windows und Microsoft Azure Active Directory mit Privileged Access Management)

Schützen des privilegierten Zugriffs

Ein Fahrplan zum Schutz Ihres privilegierten Zugriffs. Dieser Wegweiser basiert auf dem geballten Fachwissens des Teams für die Sicherheit von Servern, der Microsoft-IT, des Azure-Teams und Microsoft Consulting Services.

Just in Time Administration with Microsoft Identity Manager (Just-In-Time-Verwaltung mit Microsoft Identity Manager)

In diesem Artikel werden Features und Funktionen von Microsoft Identity Manager beschrieben. Dazu zählt auch die Unterstützung für Just-In-Time-Privileged Access Management.

Video über den Schutz von Windows und Microsoft Azure Active Directory mit privilegierter Zugriffsverwaltung

In dieser Ignite-Präsentation wird auf die Strategie und die Investitionen von Microsoft bei Windows Server, PowerShell, Active Directory, Identity Manager und Azure Active Directory eingegangen, um mithilfe einer sichereren Authentifizierung und durch die Verwaltung des Zugriffs über Just-In-Time- und Just Enough Administration-Verfahren (JEA) dem Risiko eines Administratorzugriffs entgegenzuwirken.

Artikel zu Just Enough Administration

In diesem Dokument werden die Vision und technische Details von Just Enough Administration beschrieben, einem PowerShell Toolkit, mit dem Organisationen den Administratorzugriff auf die Aufgaben beschränken können, die der jeweilige Mitarbeiter ausführen muss.

Demovideo zu Just Enough Administration

Just Enough Administration – exemplarische Vorgehensweise.

Schutz von Anmeldeinformationen

Schützen abgeleiteter Domänenanmeldeinformationen mit Credential Guard

Credential Guard nutzt auf Virtualisierung basierende Sicherheitsverfahren, um geheime Daten zu isolieren, damit nur durch privilegierte Systemsoftware auf diese Daten zugegriffen werden kann. Ein nicht autorisierter Zugriff auf diese geheimen Schlüssel kann zu Angriffen mit dem Ziel des Diebstahls von Anmeldeinformationen, z.B. Pass-the-Hash oder Pass-The-Ticket, führen. Credential Guard verhindert diese Angriffe, indem NTLM-Kennworthashes und Kerberos Ticket Granting Tickets geschützt werden.

Schützen von Remotedesktop-Anmeldeinformationen mit Remote Credential Guard

Mit Remote Credential Guard können Sie Ihre Anmeldeinformationen über eine Remotedesktopverbindung schützen, indem Kerberos-Anforderungen an das Gerät zurückgeleitet werden, das die Verbindung anfordert. Darüber hinaus profitieren Sie mit dieser Lösung von einer SSO-Umgebung (Single Sign-On, einmaliges Anmelden) für Remotedesktopsitzungen.

Demovideo zu Credential Guard

Dieses fünfminütige Video enthält Informationen über Credential Guard und Remote Credential Guard.

Ermitteln von und Reagieren auf Bedrohungen

Security Threat Analysis Using Microsoft Operations Management Suite (Analyse von Sicherheitsbedrohungen mit Microsoft Operations Management Suite)

In dieser Ignite-Präsentation wird erläutert, wie Sie Operational Insights für eine Analyse von Sicherheitsbedrohungen nutzen können.

Microsoft Operations Management Suite (OMS)

Die Sicherheits- und Überwachungslösung Microsoft Operations Management Suite (OMS) verarbeitet Sicherheitsprotokolle und Firewallereignisse aus lokalen und cloudbasierten Umgebungen, um böswilliges Verhalten zu analysieren und zu ermitteln.

Microsoft Operations Management Suite (OMS) und Windows Server

Dieses dreiminütige Video zeigt, wie OMS dabei helfen kann, potentiell böswilliges Verhalten zu erkennen, das von Windows Server blockiert wird.

Microsoft Advanced Threat Analytics

In diesem Blogbeitrag wird Microsoft Advanced Threat Analytics vorgestellt, eine lokale Lösung, die anhand von Active Directory-Netzwerkdatenverkehr und SIEM-Daten potenzielle Bedrohungen ermittelt und entsprechende Warnungen generiert.

Netzwerksicherheit

Übersicht über Datacenter Firewall

In dieser Übersicht wird Datacenter Firewall erläutert, eine zustandsbehaftete, mehrinstanzenfähige 5-Tupel-Firewall (Protokoll, Portnummer von Quelle und Ziel sowie IP-Adresse von Quelle und Ziel), die auf der Vermittlungsschicht implementiert ist.

What's New in DNS in Windows Server (Neues in DNS unter Windows Server)

In dieser Übersicht finden Sie eine kurze Beschreibung der neuen Funktionen in DNS sowie eine Reihe von Links, um auf weitere Informationen zuzugreifen.

Abbilden von Compliancebestimmungen auf Sicherheitsfunktionen

[Whitepaper zur Kompatibilitätszuordnung von abgeschirmten Hyper-V-VMs \(in englischer Sprache\)](#)

[Whitepaper zur Kompatibilitätszuordnung von JEA und JIT \(in englischer Sprache\)](#)

[Whitepaper zur Kompatibilitätszuordnung von Credential Guard \(in englischer Sprache\)](#)

[Whitepaper zur Kompatibilitätszuordnung von Credential Guard \(in englischer Sprache\)](#)

[Whitepaper zur Kompatibilitätszuordnung von Windows Defender \(in englischer Sprache\)](#)

Starten ihrer Datenschutz-Grundverordnung-Journey (dsgvo) für Windows Server

15.01.2020 • 70 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieser Artikel enthält Informationen zu den GDPR, einschließlich einer Beschreibung und der Produkte von Microsoft, um Ihnen den Einstieg in die Kompatibilität zu erleichtern.

Einführung

Am 25. Mai 2018 tritt ein europäisches Datenschutzgesetz in Kraft, das ein neues globales Niveau für Datenschutz, Sicherheit und Compliance festlegt.

Die allgemeine Data Protection-Richtlinie, oder GDPR, ist im Grunde über Schutz und Aktivierung des Datenschutzrechts von Personen. Die GDPR stellt strikte globale Datenschutzanforderungen über die Verwaltung und den persönlichen Schutz von Daten bei gleichzeitiger Wahrung der Auswahl des Individuums – unabhängig davon, wo die Daten gesendet, verarbeitet oder gespeichert werden.

Microsoft und unsere Kunden bemühen sich aktuell, die Ziele des Datenschutzes der GDPR zu erzielen. Wir von Microsoft sind der Meinung, Datenschutz ist ein grundlegendes Recht, und wir glauben, dass die GDPR ein wichtiger Schritt für den Schutz und die Aktivierung des Datenschutzrechts von Personen ist. Aber wir wissen auch, dass eine GDPR wichtige Änderungen bei Organisationen weltweit erfordert.

Wir haben unser Engagement für die GDPR beschrieben und wie wir unsere Kunden unterstützen. Diese finden Sie in dem Blogbeitrag [Mit Microsoft-Cloud GDPR-kompatibel werden](#) von unseren Chief Privacy Officer [Brendon Lynch](#) und dem Blogbeitrag [Sichern Sie Ihre Vertrauensstellung mit vertraglichen Verpflichtungen für die allgemeine Data Protection Verordnung](#) von [Rich Sauer](#) - Microsoft Corporate Vice President & Deputy General Counsel.

Auch wenn Ihrer Reise in die GDPR-Kompatibilität eine große Herausforderung zu sein scheint, wir sind hier, um Sie zu unterstützen. Spezifische Informationen über die GDPR, unsere Verpflichtungen und wie Sie Ihre Reise beginnen finden Sie im [GDPR-Abschnitt im Microsoft Trust Center](#).

GDPR und seine Folgen

Der GDPR ist eine komplexe Verordnung, die möglicherweise wesentliche Änderungen in Bezug auf das Sammeln, Verwenden und Verwalten von persönlichen Daten erfordert. Microsoft hilft seit langem seinen Kunden komplexe Bestimmungen zu befolgen, und bei der Vorbereitung auf den GDPR sind wir Ihr Partner auf dem Weg.

GDPR erzwingt Regeln für Organisationen, die Waren anbieten und an Personen in der Europäischen Union (EU) verkaufen, oder die Daten für Mitglieder der EU sammeln und analysieren, unabhängig davon, wo sich diese Unternehmen befinden. Im Folgenden finden Sie die Schlüsselemente der GDPR:

- **Erweiterte persönliche Datenschutz Rechte.** Ein stärkerer Datenschutz für Einwohner der EU, um sicherzustellen, dass sie die Zugriffsberechtigung für den Zugriff auf ihre persönlichen Daten erhalten, Ungenauigkeiten in diesen Daten korrigieren, diese löschen können, bei der Verarbeitung ihrer persönlichen Daten Einspruch erheben und diese verschieben können.
- **Erhöhung der Aufgaben zum Schutz personenbezogener Daten.** Verstärkte Verantwortlichkeit von Organisationen, die personenbezogene Daten verwalten, mehr Klarheit der Verantwortung bei der

Einhaltung der Kompatibilität.

- **Obligatorische Berichte zu personenbezogenen Datenverletzungen.** Organisationen, die Kontrolle über persönliche Daten haben müssen ihren zuständigen Behörden unverzüglich persönliche Datenverstöße melden, die die Rechte und Grundfreiheiten von Personen gefährden, und wenn möglich innerhalb von 72 Stunden nachdem die Verletzung bekannt wird.

Wie erwartet hat die GDPR einen erheblichen Einfluss auf Ihr Unternehmen und erfordert eventuell die Datenschutzrichtlinien zu aktualisieren, Datenschutzkontrollen und -verstoßprozeduren zu implementieren und zu stärken, transparente Richtlinien bereitzustellen und in IT und Schulungen weite zu investieren. Mit Microsoft Windows 10 können Sie effektiv und effizient einige der folgenden Anforderungen in den Griff bekommen.

Persönliche und vertrauliche Daten

Als Teil Ihres Aufwands zur Einhaltung der GDPR müssen Sie wissen, wie Verordnung persönliche und vertrauliche Daten definiert und wie diese Definitionen auf Daten Ihrer Organisation zutrifft. Basierend auf diesem Verständnis können Sie ermitteln, wo diese Daten erstellt, verarbeitet, verwaltet und gespeichert werden.

Die GDPR betrachtet persönliche Daten als alle Informationen im Zusammenhang mit einer bestimmten oder bestimmbarer natürlichen Person. Dies bedeutet eine direkte Identifizierung (z. B. Ihr vollständiger Name) und eine indirekte Identifizierung (z. B. bestimmte Informationen, die Sie als Datenverweis identifiziert). Die GDPR verdeutlicht, dass das Konzept der persönlichen Daten Online-IDs (z. B. IP-Adressen, mobile Geräte-IDs) und Positionsdaten umfasst.

Die DSGVO führt bestimmte Definitionen für die Daten der genetische Daten (z. B. die Gene Rate eines Einzelpersonen) und biometrische Daten ein. Genetische Daten und biometrische Daten zusammen mit anderen Unterkategorien persönlicher Daten (persönliche Daten Offenlegung von rassischem oder ethnischen Ursprung, politischen Meinungen, religiösen oder philosophischen Überzeugungen oder Mitgliedschafts Mitgliedschaften: Daten zur Integrität oder Daten zu einem das Geschlecht der Person oder die sexuelle Orientierung) werden als sensible personenbezogene Daten in der DSGVO behandelt. Sensible personenbezogene Daten bieten erweiterten Schutz und erfordern im Allgemeinen die explizite Zustimmung eines einzelnen, wenn diese Daten verarbeitet werden sollen.

Beispiele für Informationen über eine bestimmte oder bestimmbarer natürliche Person (Datenbetreff)

Diese Liste enthält Beispiele für verschiedene Arten von Informationen, die über GDPR geregelt werden. Diese Liste ist nicht vollständig.

- Name
- ID-Nummer (wie Sozialversicherungsnummer)
- Wohnortdaten (z. B. die Privatadresse)
- Online-ID (z. B. die E-Mail-Adresse, der Bildschirmname, die IP-Adresse, Geräte-IDs)
- Pseudonyme Daten (z. B. einen Schlüssel zur Personenidentität verwenden)
- Genetische Daten (z. B. biologische Stichproben einer Person)
- Biometrische Daten (z. B. Fingerabdrücke, Gesichtserkennung)

Erste Schritte auf dem Weg in Richtung GDPR-Kompatibilität

Da der Schritt zur GDPR-Kompatibilität vieles umfasst, wird dringend empfohlen, mit den Vorbereitungen nicht bis zum Erzwingen der Richtlinien zu warten. Sie sollten Ihre Privatsphäre- und die Daten-Verwaltungsverfahren jetzt überprüfen. Es wird empfohlen, dass Sie Ihre Reise in die GDPR-Kompatibilität durch den Fokus auf vier wichtige Schritte beginnen:

- **Stellen.** Identifizieren Sie Ihre persönlichen Daten und wo sie sich befinden.
- **Stelligen.** Steuern, wie auf persönliche Daten zugegriffen und wie sie verwendet werden.
- **Schützen.** Richten Sie Sicherheitsmechanismen ein, um zu verhindern, erkennen und auf Sicherheitsrisiken und Datenschutzverletzungen zu reagieren.
- **Ver.** Reagieren Sie auf Datenanforderungen, melden Sie Datenschutzverletzungen, und behalten Sie die erforderliche Dokumentation.



Für die einzelnen Schritte haben wir Beispiel-Tools, Ressourcen und Funktionen in verschiedenen Microsoft-Lösungen beschrieben, die verwendet werden können, um die Anforderungen des Schritts einzuhalten. Dieser Artikel ist zwar kein umfassendes Leitfadens, aber wir haben Links für Sie eingefügt, um weitere Informationen zu erhalten. Weitere Informationen finden Sie im Abschnitt zur dsgvo im [Microsoft Trust Center](#).

Sicherheit und Datenschutz für Windows Server

Die dsgvo erfordert, dass Sie geeignete technische und organisatorische Sicherheitsmaßnahmen implementieren, um persönliche Daten und Verarbeitungssysteme zu schützen. Im Zusammenhang mit der dsgvo verarbeiten Ihre physischen und virtuellen Serverumgebungen möglicherweise persönliche und vertrauliche Daten. Die Verarbeitung kann jeden Vorgang oder jede Gruppe von Vorgängen, z. b. Datenerfassung, Speicherung und Abruf, bedeuten.

Die Möglichkeit, diese Anforderung zu erfüllen und geeignete Maßnahmen für die technische Sicherheit zu implementieren, muss die Bedrohungen widerspiegeln, die Ihnen in der zunehmend feindlichen IT-Umgebung von heute ausgesetzt sind. Die heutige Sicherheits-Bedrohungslandschaft ist eine der aggressiven und hartnäckigen Bedrohungen. In früheren Jahren konzentrierten sich böswillige Angreifer hauptsächlich auf die Anerkennung in der Community für ihre Angriffe oder die Begeisterung, ein System vorübergehend offline geschaltet zu haben. Seitdem haben sich die Gründe für den Angreifer auf Geld verlagert, einschließlich der Speicherung von Geräten und Daten, bis der Besitzer das geforderte Lösegeld bezahlt hat.

Aktuelle Angriffe konzentrieren sich zunehmend auf den Diebstahl geistigen Eigentums im großen Umfang, die zielgerichtete Systemzersetzung, die zu finanziellen Verlusten führen kann, und jetzt sogar Cyber-Terrorismus, durch den die Sicherheit von Personen und Unternehmen sowie nationale Interessen auf der ganzen Welt bedroht sind. Diese Angreifer sind üblicherweise hochqualifizierte Einzelpersonen und Sicherheitsexperten, von denen einige in Nationalstaaten beschäftigt sind, die über große Budgets und scheinbar unbegrenzte menschliche Ressourcen verfügen. Bedrohungen wie diese erfordern einen Ansatz, der dieser Herausforderung gerecht wird.

Diese Bedrohungen sind nicht nur ein Risiko für Ihre Fähigkeit, die Kontrolle über persönliche oder vertrauliche Daten zu behalten, sondern sie sind ein wesentliches Risiko für Ihr gesamtes Unternehmen. Beachten Sie die neuesten Daten von McKinsey, Ponemon Institute, Verizon und Microsoft:

- Die durchschnittliche Kosten für den Typ der Datenverstöße, den die GDPR erwartet, beträgt 3,5 Milliarden USD.

- 63 % dieser Verstößen sind schwache oder gestohlene Kennwörter, mit denen Sie handeln müssen und die die GDPR erwartet.
- Über 300.000 neue Schadsoftware-Beispiele werden jeden Tag erstellt und verbreitet und machen Ihre Aufgabe des Schutzes von Daten noch schwieriger.

Wie bei den jüngsten Ransomware-Angriffen, die einmal als schwarze Plage des Internets bezeichnet werden, werden Angreifer nach größeren Zielen weitergegeben, die sich möglicherweise mit schwerwiegenden Konsequenzen beschäftigen können. Die DSGVO schließt Maßnahmen ein, die ihre Systeme, einschließlich Desktops und Laptops, zur Verfügung stellen, die tatsächlich persönliche und sensible datenreiche Ziele enthalten.

Zwei wichtige Prinzipien haben eine Anleitung und Fortsetzung bei der Entwicklung von Windows:

- **Sicherheit.** Die Daten unsere Software und Dienste im Auftrag unserer Kunden sollten vor Schäden geschützt werden und werden nur auf angemessene Weise verwendet oder geändert. Sicherheitsmodelle sollten Entwicklern auf einfache Weise vertraut sein, um Ihre Anwendungen zu verstehen und zu erstellen.
- **Datenschutz.** Benutzer sollten Steuern, wie Ihre Daten verwendet werden. Die Richtlinien für die Verwendung von Informationen sollten für den Benutzer klar sein. Benutzer sollten steuern können, wann und ob Sie Informationen erhalten, um Ihre Zeit optimal zu nutzen. Es sollte einfach sein, dass Benutzer die geeignete Verwendung Ihrer Informationen angeben können, einschließlich der Steuerung der Verwendung von gesendeten e-Mails.

Microsoft hat sich im Hinblick auf diese Prinzipien nicht wie vor kurzem vom CEO von Microsoft, Satya NADELLA,

"Wenn sich die Welt weiter ändert und sich die geschäftlichen Anforderungen weiterentwickeln, sind einige Dinge konsistent: die Nachfrage nach Sicherheit und Datenschutz durch einen Kunden."

Bei der Einhaltung der DSGVO ist es wichtig, die Rolle ihrer physischen und virtuellen Server beim Erstellen, zugreifen, verarbeiten, speichern und Verwalten von Daten zu verstehen, die als persönliche und potenziell sensible Daten in der DSGVO qualifiziert sein können. Windows Server bietet Funktionen, mit deren Hilfe Sie die DSGVO-Anforderungen erfüllen können, um geeignete technische und organisatorische Sicherheitsmaßnahmen zum Schutz persönlicher Daten zu implementieren.

Die Sicherheitslage von Windows Server 2016 ist kein Bolt-on. Es ist ein Architekturprinzip. Und Sie können in vier Prinzipale am besten verstanden werden:

- **Schützen.** Fortlaufender Fokus und Innovation bei präventiven Maßnahmen blockieren bekannter Angriffe und bekannter Schadsoftware.
- **Auf.** Umfassende Überwachungstools, die Sie dabei unterstützen, Abweichungen zu erkennen und schneller auf Angriffe zu reagieren.
- **Reagieren.** Führende Antwort- und Wiederherstellungs Technologien sowie Deep Consulting-Know-how.
- **Isol.** Isolieren Sie Betriebssystemkomponenten und Daten Geheimnisse, schränken Sie Administratorrechte ein, und Messen Sie die Host Integrität streng.

Mit Windows Server ist die Fähigkeit, die Arten von Angriffen zu schützen, zu erkennen und zu schützen, die zu Datenverletzungen führen können, erheblich verbessert. Angesichts der strengen Anforderungen hinsichtlich der Verletzung der Benachrichtigung innerhalb der GDPR, und um sicherzustellen, dass Ihre Desktop- und Laptop-Systeme auch gegen Risiken gesichert sind, verringern Sie das Risiko kostspieliger Verletzungsanalysen und Benachrichtigungen.

Im folgenden Abschnitt erfahren Sie, wie Windows Server Funktionen bereitstellt, die sich in der Phase "schützen" ihrer DSGVO-Kompatibilitäts Journey ganz direkt befinden. Diese Funktionen fallen in drei Schutz Szenarien:

- **Schützen Sie Ihre Anmelde Informationen, und beschränken Sie Administratorrechte.** Windows

Server 2016 hilft bei der Implementierung dieser Änderungen, um zu verhindern, dass Ihr System als Ausgangspunkt für weitere Eindring Versuche verwendet wird.

- **Sichern Sie das Betriebssystem, um Ihre apps und die Infrastruktur auszuführen.** Windows Server 2016 bietet Schutz Ebenen, die verhindern, dass externe Angreifer Schadsoftware ausführen oder Sicherheitsrisiken ausnutzen.
- **Sichere Virtualisierung.** Windows Server 2016 ermöglicht die sichere Virtualisierung mit abgeschirmten Virtual Machines und geschütztem Fabric. Dies hilft Ihnen, Ihre virtuellen Computer auf vertrauenswürdigen Hosts in Ihrem Fabric zu verschlüsseln und auszuführen, um Sie besser vor böswilligen Angriffen zu schützen.

Diese Funktionen, die unten ausführlicher erläutert werden, mit Verweisen auf bestimmte dsgvo-Anforderungen, basieren auf dem erweiterten Geräteschutz, der die Integrität und Sicherheit des Betriebssystems und der Daten gewährleistet.

Eine Schlüssel Bereitstellung innerhalb der dsgvo ist der Schutz von Daten nach Entwurf und standardmäßig, und unterstützt Sie bei der Erfüllung dieser Bereitstellung in Windows 10, wie z. b. der BitLocker-Geräteverschlüsselung. BitLocker verwendet die Trusted Platform Module (TPM)-Technologie, die hardwarebasierte, sicherheitsrelevante Funktionen bereitstellt. Dieser kryptografieprozessorchip umfasst mehrere physische Sicherheitsmechanismen, um ihn zu manipulieren, und Schadsoftware kann die Sicherheitsfunktionen des TPM nicht manipulieren.

Der Chip umfasst mehrere physische Sicherheitsmechanismen, die ihn manipulationssicher machen, und Schadsoftware ist nicht in der Lage, die Sicherheitsfunktionen des TPMs zu manipulieren. Die wichtigsten Vorteile der TPM-Technologie bestehen in ihren Möglichkeiten. Sie können:

- Kryptografieschlüssel generieren, speichern und deren Einsatz beschränken.
- Verwenden Sie die TPM-Technologie für die Plattform Geräte Authentifizierung, indem Sie den eindeutigen TPM-RSA-Schlüssel verwenden, der in sich selbst gebrannt wird.
- Plattformintegrität gewährleisten, indem Sicherheitsmessungen vorgenommen und gespeichert werden.

Zusätzliche erweiterte Schutzmaßnahmen für Ihr Betriebssystem ohne Datenschutzverletzungen umfassen „Windows Trusted Boot“, das die Integrität des Systems gewährleistet, indem es sicherstellt, dass die Schadsoftware nicht vor den Verteidigungseinrichtungen des Systems gestartet werden kann.

Windows Server: Unterstützung ihrer dsgvo-Konformitäts Journey

Wichtige Features in Windows Server können Sie bei der effizienten und effektiven Implementierung der Sicherheits- und Datenschutzmechanismen unterstützen, die für die Einhaltung der dsgvo erforderlich sind. Obwohl die Verwendung dieser Features nicht die Konformität gewährleistet, unterstützen Sie Ihre Bemühungen, dies zu tun.

Das Server Betriebssystem befindet sich in einer strategischen Schicht in der Infrastruktur einer Organisation und bietet neue Möglichkeiten, Schutz Ebenen vor Angriffen zu schaffen, die Daten stehlen und Ihr Unternehmen unterbrechen könnten. Wichtige Aspekte der dsgvo, wie z. b. Datenschutz, Datenschutz und Access Control müssen innerhalb Ihrer IT-Infrastruktur auf Serverebene adressiert werden.

Windows Server 2016 trägt zum Schutz der Identitäts-, Betriebssystem- und Virtualisierungsebene bei, um die häufigen Angriffsvektoren zu blockieren, die für den unerlaubten Zugriff auf Ihre Systeme verwendet werden: gestohlene Anmelde Informationen, Schadsoftware und ein kompromittiertes virtualisierungsfabric. Zusätzlich zu den Sicherheitsrisiken, die in Windows Server 2016 integriert sind, unterstützen die Sicherheitskomponenten, die in Windows Server integriert sind, Compliance-Anforderungen für die wichtigsten behördlichen

Diese Identitäts-, Betriebssystem- und virtualisierungsschutzmaßnahmen ermöglichen es Ihnen, Ihr Rechenzentrum mit Windows Server als virtuellen Computer in einer beliebigen Cloud zu schützen und die Fähigkeit von

Angreifern einzuschränken, Anmelde Informationen zu kompromittieren, Schadsoftware zu starten und nicht erkannt zu werden. Netzwerk. Ebenso bietet Windows Server 2016 bei der Bereitstellung als Hyper-V-Host eine Sicherheitsgarantie für Ihre Virtualisierungsumgebungen durch geschützte Virtual Machines und verteilte Firewallfunktionen. Mit Windows Server 2016 wird das Server Betriebssystem zu einem aktiven Teilnehmer in ihrer Datacenter-Sicherheit.

Schützen Sie Ihre Anmelde Informationen, und beschränken Sie Administratorrechte.

Die Kontrolle über den Zugriff auf personenbezogene Daten und die Systeme, die diese Daten verarbeiten, ist ein Bereich mit der DSGVO, der bestimmte Anforderungen umfasst, einschließlich des Zugriffs durch Administratoren. Privilegierte Identitäten sind Konten mit erhöhten Rechten, wie z. B. Benutzerkonten, die Mitglieder der Gruppe "Domänen Administratoren", "Organisations Administratoren", "lokale Administratoren" oder "Hauptbenutzer" sind. Diese Identitäten können auch Konten enthalten, denen direkt Berechtigungen erteilt wurden, z. B. das Ausführen von Sicherungen, das Herunterfahren des Systems oder andere Rechte, die im Knoten zuweisen von Benutzerrechten in der Konsole der lokalen Sicherheitsrichtlinie aufgeführt sind.

Als allgemeines Zugriffs Steuerungs Prinzip und Inline mit der DSGVO müssen Sie diese privilegierten Identitäten vor Kompromittierung durch potenzielle Angreifer schützen. Zuerst ist es wichtig zu verstehen, wie Identitäten kompromittiert werden. Anschließend können Sie planen, um zu verhindern, dass Angreifer Zugriff auf diese privilegierten Identitäten erhalten.

Wie werden privilegierte Identitäten kompromittiert?

Privilegierte Identitäten können kompromittiert werden, wenn Organisationen nicht über Richtlinien zum Schutz verfügen. Im Folgenden finden Sie entsprechende Beispiele:

- **Mehr Berechtigungen als erforderlich sind.** Eines der häufigsten Probleme besteht darin, dass Benutzer über mehr Berechtigungen verfügen, als für die Ausführung ihrer Auftrags Funktion erforderlich sind. Beispielsweise kann ein Benutzer, der DNS verwaltet, ein AD-Administrator sein. In den meisten Fällen wird dies durchgeführt, um zu vermeiden, dass unterschiedliche Verwaltungsebenen konfiguriert werden müssen. Wenn ein solches Konto jedoch kompromittiert wird, hat der Angreifer automatisch erhöhte Rechte.
- **Ständig mit erhöhten Rechten angemeldet.** Ein weiteres häufiges Problem ist, dass Benutzer mit erhöhten Rechten diese für unbegrenzte Zeit verwenden können. Dies gilt sehr häufig für IT-Experten, die sich mit einem privilegierten Konto bei einem Desktop Computer anmelden, angemeldet bleiben und das privilegierte Konto zum Durchsuchen des Internets und zum Verwenden von e-Mails verwenden (typische IT-Arbeitsaufgaben Funktionen). Durch die unbegrenzte Dauer privilegierter Konten ist das Konto anfälliger für Angriffe und erhöht die Wahrscheinlichkeit, dass das Konto gefährdet wird.
- **Social Engineering Research.** Die meisten Bedrohungen der Anmelde Informationen beginnen mit der Untersuchung der Organisation und Durchführung durch Social Engineering. Beispielsweise kann ein Angreifer einen e-Mail-Phishing-Angriff durchführen, um legitime Konten (aber nicht unbedingt Konten mit erhöhten Rechten) zu kompromittieren, die Zugriff auf das Netzwerk einer Organisation haben. Der Angreifer verwendet dann diese gültigen Konten, um zusätzliche Untersuchungen in Ihrem Netzwerk durchzuführen und privilegierte Konten zu identifizieren, die administrative Aufgaben ausführen können.
- **Nutzen Sie Konten mit erhöhten Rechten.** Selbst bei einem normalen, nicht erhöhten Benutzerkonto im Netzwerk können Angreifer Zugriff auf Konten mit erhöhten Berechtigungen erhalten. Eine der gängigeren Methoden hierfür ist die Verwendung der Pass-the-Hash-oder Pass-the-Token-Angriffe. Weitere Informationen zu den Verfahren Pass-the-Hash und andere Verfahren zum Diebstahl von Anmelde Informationen finden Sie in den Ressourcen auf der [Seite Pass-the-Hash \(PTH\)](#).

Es gibt natürlich andere Methoden, mit denen Angreifer privilegierte Identitäten identifizieren und kompromittieren können (wobei täglich neue Methoden erstellt werden). Daher ist es wichtig, dass Sie Verfahren für Benutzer einrichten, die sich mit Konten mit geringsten Berechtigungen anmelden, um die Möglichkeit zu verringern, dass Angreifer Zugriff auf privilegierte Identitäten erhalten. In den folgenden Abschnitten werden die Funktionen beschrieben, mit denen Windows Server diese Risiken mindern kann.

Just-in-time admin (JIT) und Just Enough admin (Jea)

Obwohl der Schutz vor Pass-the-Hash-oder Pass-The-Ticket-Angriffen wichtig ist, können Administrator Anmelde Informationen weiterhin auf andere Weise gestohlen werden, einschließlich Social Engineering, verärgerten Employees und Brute-Force. Daher ist es nicht nur so weit wie möglich, Anmelde Informationen zu isolieren, sondern auch die Reichweite von Berechtigungen auf Administratorebene einzuschränken, falls diese kompromittiert sind.

Heute sind zu viele Administrator Konten überlastet, auch wenn Sie nur einen Zuständigkeitsbereich haben. Beispielsweise werden einem DNS-Administrator, der einen sehr schmalen Satz von Berechtigungen zum Verwalten von DNS-Servern benötigt, häufig Berechtigungen auf Administratorebene erteilt. Außerdem gibt es keine Beschränkung, wie lange Sie verwendet werden können, da diese Anmelde Informationen für die Dauerhaftigkeit erteilt werden.

Jedes Konto mit unnötigen Berechtigungen auf Domänen Administratorebene erhöht die Angriffsfläche für Angreifer, die Anmelde Informationen kompromittieren möchten. Um die Angriffsfläche für Angriffe zu minimieren, sollten Sie nur den spezifischen Satz von rechten bereitstellen, den ein Administrator für den Auftrag benötigt – und nur für das Zeitfenster, das zum Abschluss benötigt wird.

Mithilfe der eben ausreichenden Administration und Just-in-Time-Verwaltung können Administratoren die spezifischen Berechtigungen anfordern, die Sie für das genaue Zeitfenster benötigen, das benötigt wird. Für einen DNS-Administrator können Sie z. B. mithilfe von PowerShell nur eine ausreichende Verwaltung aktivieren, um einen begrenzten Satz von Befehlen zu erstellen, die für die DNS-Verwaltung verfügbar sind.

Wenn der DNS-Administrator einen Ihrer Server aktualisieren muss, fordert er den Zugriff zum Verwalten von DNS mithilfe von Microsoft Identity Manager 2016 an. Der Anforderungs Workflow kann einen Genehmigungsprozess einschließen, z. B. die zweistufige Authentifizierung, bei dem das Mobiltelefon des Administrators aufgerufen werden kann, um Ihre Identität zu bestätigen, bevor die angeforderten Berechtigungen erteilt werden. Nach der Erteilung gewähren diese DNS-Berechtigungen den Zugriff auf die PowerShell-Rolle für DNS für eine bestimmte Zeitspanne.

Stellen Sie sich dieses Szenario vor, wenn die Anmelde Informationen des DNS-Administrators gestohlen wurden. Da den Anmelde Informationen keine Administratorrechte zugeordnet sind, konnte der Angreifer zunächst nicht auf den DNS-Server – oder andere Systeme – zugreifen, um Änderungen vorzunehmen. Wenn der Angreifer versucht hat, Berechtigungen für den DNS-Server anzufordern, werden Sie von der zweistufigen Authentifizierung aufgefordert, Ihre Identität zu bestätigen. Da der Angreifer wahrscheinlich nicht über das Mobiltelefon des DNS-Administrators verfügt, schlägt die Authentifizierung fehl. Dadurch wird der Angreifer vom System gesperrt und die IT-Organisation benachrichtigt, dass die Anmelde Informationen kompromittiert werden könnten.

Außerdem verwenden viele Organisationen die kostenlose [lokale Administrator Kenn Wort Lösung \(Runden\)](#) als einfachen, aber leistungsfähigen JIT-Verwaltungsmechanismus für Ihre Server-und Client Systeme. Die Runden Funktion ermöglicht die Verwaltung von lokalen Konto Kennwörtern für in die Domäne eingebundener Computer. Kenn Wörter werden in Active Directory (AD) gespeichert und von Access Control Liste (ACL) geschützt, sodass nur berechtigte Benutzer Sie lesen oder deren zurück Setzung anfordern können.

Wie im Leitfaden zur [Entschärfung von Windows](#)-Anmelde Informationen vermerkt,

"die Tools und Techniken, die kriminelle zum Durchführen von Diebstahl von Anmelde Informationen und zum wieder verwenden von Angriffen verwenden, werden durch böswillige Angreifer leichter gefunden. Der Diebstahl von Anmelde Informationen basiert häufig auf Betriebspraktiken oder dem verfügbar machen von Benutzer Anmelde Informationen, sodass effektive entschärfungen einen ganzheitlichen Ansatz erfordern, der Personen, Prozesse und Technologien adressiert. Außerdem beruhen diese Angriffe darauf, dass der Angreifer Anmelde Informationen stiehlt, nachdem ein System zum Erweitern oder beibehalten des Zugriffs kompromittiert wurde, sodass Organisationen rasch Verletzungen durch Implementieren von Strategien aufweisen müssen, die verhindern, dass Angreifer in einem gefährdeten Netzwerk frei und unentdeckt bleiben.

"

Eine wichtige Entwurfs Überlegungen für Windows Server bestand darin, den Diebstahl von Anmelde Informationen zu mindern – insbesondere abgeleitete Anmelde Informationen. Anmelde Informationen Guard bietet eine deutlich verbesserte Sicherheit vor dem Diebstahl und der Wiederverwendung abgeleiteter Anmelde Informationen, indem eine bedeutende Architektur Änderung in Windows implementiert wurde, um hardwarebasierte Isolations Angriffe auszuschließen, anstatt einfach zu versuchen, gegen Sie schützen.

Bei der Verwendung von Windows Defender Anmelde Informationen Guard, NTLM und Kerberos abgeleitete Anmelde Informationen werden mithilfe der virtualisierungsbasierten Sicherheit geschützt, aber die Verfahren und Tools zum Diebstahl von Anmelde Informationen, die in vielen gezielten Angriffen verwendet werden, werden blockiert. Im Betriebssystem ausgeführte Schadsoftware mit Administratorberechtigungen kann geheime Schlüssel, die durch die virtualisierungsbasierte Sicherheit geschützt sind, nicht extrahieren. Obwohl Windows Defender Credential Guard eine leistungsstarke Entschärfung ist, werden permanente Bedrohungs Angriffe wahrscheinlich zu neuen Angriffstechniken verschoben, und Sie sollten auch Device Guard, wie unten beschrieben, zusammen mit anderen Sicherheitsstrategien und-Architekturen integrieren.

Windows Defender Credential Guard

Windows Defender Anmelde Informationen Guard verwendet virtualisierungsbasierte Sicherheit, um Anmelde Informationen zu isolieren, sodass Kennworthashes oder Kerberos-Tickets nicht abgefangen werden. Er verwendet einen völlig neuen, isolierten lokalen Sicherheits Autorität (Local Security Authority, LSA), der für den Rest des Betriebssystems nicht zugänglich ist. Alle Binärdateien, die von der isolierten LSA verwendet werden, werden mit Zertifikaten signiert, die überprüft werden, bevor Sie in der geschützten Umgebung gestartet werden, sodass Pass-the-Hash-Typen Angriffe vollständig wirkungslos werden.

Windows Defender Credential Guard verwendet Folgendes:

- Virtualisierungsbasierte Sicherheit (erforderlich). Ebenfalls erforderlich:
 - 64-Bit-CPU
 - Erweiterungen der CPU-Virtualisierung sowie erweiterte Seitentabellen
 - Windows-Hypervisor
- Sicherer Start (erforderlich)
- TPM 2.0, entweder diskret oder firmwarebasiert (aufgrund der Hardwarebindung bevorzugt)

Sie können Windows Defender Anmelde Informationen Guard verwenden, um privilegierte Identitäten zu schützen, indem Sie die Anmelde Informationen und die Ableitungen von Anmelde Informationen unter Windows Server 2016 schützen. Weitere Informationen zu den Anforderungen von Windows Defender Credential Guard finden Sie unter [schützen abgeleiteter Domänen Anmelde Informationen mit Windows Defender Credential Guard](#).

Windows Defender Remote Credential Guard

Windows Defender Remote Credential Guard unter Windows Server 2016 und Windows 10 Anniversary Update unterstützt auch den Schutz von Anmelde Informationen für Benutzer mit Remote Desktop Verbindungen. Zuvor musste sich jede Person, die Remotedesktopdienste verwendet, bei Ihrem lokalen Computer anmelden und sich dann erneut anmelden, wenn Sie eine Remote Verbindung mit dem Zielcomputer durchgeführt hat. Dieser zweite Anmelde Name übergibt Anmelde Informationen an den Zielcomputer und macht Sie für Pass-the-Hash-oder Pass-The-Ticket-Angriffe verfügbar.

Mit Windows Defender Remote Credential Guard implementiert Windows Server 2016 Single Sign-on für Remotedesktop Sitzungen, sodass der Benutzername und das Kennwort nicht erneut eingegeben werden müssen. Stattdessen werden die Anmelde Informationen verwendet, die Sie bereits zum Anmelden an Ihrem lokalen Computer verwendet haben. Um Windows Defender Remote Credential Guard verwenden zu können, müssen die Remotedesktop Client und der Server die folgenden Anforderungen erfüllen:

- Muss einer Active Directory Domäne beitreten und sich in derselben Domäne oder in einer Domäne mit einer Vertrauensstellung befinden.

- Muss die Kerberos-Authentifizierung verwenden.
- Muss mindestens Windows 10, Version 1607 oder Windows Server 2016 ausführen.
- Die Remotedesktop klassische Windows-APP ist erforderlich. Die Remotedesktop universelle Windows-Plattform-App unterstützt nicht Windows Defender Remote Credential Guard.

Sie können Windows Defender Remote Credential Guard aktivieren, indem Sie eine Registrierungs Einstellung auf dem Remotedesktop Server und Gruppenrichtlinie oder einen Remotedesktopverbindung Parameter auf dem Remotedesktop Client verwenden. Weitere Informationen zum Aktivieren von Windows Defender Remote Credential Guard finden Sie unter [Schützen von Remotedesktop Anmelde Informationen mit Windows Defender Remote Credential Guard](#). Wie bei Windows Defender Credential Guard können Sie Windows Defender Remote Credential Guard verwenden, um privilegierte Identitäten unter Windows Server 2016 zu schützen.

Sichern des Betriebssystems zum Ausführen von apps und Infrastrukturen

Das Verhindern von Cyberbedrohungen erfordert auch das Auffinden und Blockieren von Schadsoftware und Angriffen, die die Kontrolle über die Standard Betriebssysteme Ihrer Infrastruktur erlangen. Wenn Angreifer ein Betriebssystem oder eine Anwendung für die Ausführung in einer nicht vordefinierten, nicht realisierbaren Weise erhalten können, verwenden Sie wahrscheinlich dieses System, um böswillige Aktionen auszuführen. Windows Server 2016 bietet Schutz Ebenen, die verhindern, dass externe Angreifer Schadsoftware ausführen oder Sicherheitsrisiken ausnutzen. Das Betriebssystem übernimmt eine aktive Rolle beim Schutz von Infrastruktur und Anwendungen, indem Administratoren auf Aktivitäten hingewiesen werden, die darauf hindeuten, dass ein System verletzt wurde.

Windows Defender Device Guard

Windows Server 2016 enthält Windows Defender Device Guard, um sicherzustellen, dass nur vertrauenswürdige Software auf dem Server ausgeführt werden kann. Mithilfe der virtualisierungsbasierten Sicherheit kann durch die IT-Abteilung eingeschränkt werden, welche Binärdateien auf dem System basierend auf der Richtlinie der Organisation ausgeführt werden können. Wenn etwas anderes als die angegebenen Binärdateien ausgeführt werden soll, wird es von Windows Server 2016 blockiert, und der fehlgeschlagene Versuch wird protokolliert, damit Administratoren erkennen können, dass eine potenzielle Verletzung aufgetreten ist. Die Warnungs Benachrichtigung ist ein wichtiger Bestandteil der Anforderungen hinsichtlich der Einhaltung der DSGVO.

Windows Defender Device Guard ist auch in PowerShell integriert, sodass Sie autorisieren können, welche Skripts auf Ihrem System ausgeführt werden können. In früheren Versionen von Windows Server konnten Administratoren die Code Integritäts Erzwingung umgehen, indem Sie einfach die Richtlinie aus der Codedatei löschen. Mit Windows Server 2016 können Sie eine Richtlinie konfigurieren, die von Ihrer Organisation signiert wird, sodass nur eine Person mit Zugriff auf das Zertifikat, mit dem die Richtlinie signiert wurde, die Richtlinie ändern kann.

Ablaufsteuerungsschutz

Windows Server 2016 umfasst auch integrierten Schutz gegen einige Klassen von Speicher Beschädigungen. Das Patchen Ihrer Server ist wichtig, aber es besteht immer die Möglichkeit, dass Schadsoftware für ein Sicherheitsrisiko entwickelt wird, das noch nicht identifiziert wurde. Einige der gängigsten Methoden zum Ausnutzen dieser Sicherheitsrisiken sind die Bereitstellung ungewöhnlicher oder extremer Daten für ein ausgelaufenes Programm. Ein Angreifer kann z. B. ein Pufferüberlauf-Sicherheitsrisiko ausnutzen, indem er mehr Eingaben für ein Programm als erwartet bereitstellt und den vom Programm reservierten Bereich zum Speichern einer Antwort überschreitet. Dadurch kann der angrenzende Arbeitsspeicher beschädigt werden, der möglicherweise einen Funktionszeiger enthält.

Wenn das Programm diese Funktion aufruft, kann es zu einem unbeabsichtigten Speicherort springen, der vom Angreifer angegeben wird. Diese Angriffe werden auch als Jump-Oriented Programming-Angriffe (jop) bezeichnet. Der Ablauf Steuerungs Schutz verhindert Jop-Angriffe, indem strenge Einschränkungen für den Anwendungscode festgelegt werden, – insbesondere indirekte Aufrufe. Es werden vereinfachte Sicherheitsüberprüfungen hinzugefügt, um den Satz von Funktionen in der Anwendung zu identifizieren, die gültige Ziele für indirekte Aufrufe

sind. Wenn eine Anwendung ausgeführt wird, überprüft Sie, ob diese indirekten Callziele gültig sind.

Wenn bei der Überprüfung des Ablaufsteuerungsschutzes zur Laufzeit ein Fehler auftritt, beendet Windows Server 2016 das Programm sofort und unterbricht alle Exploits, die versuchen, indirekt eine ungültige Adresse aufzurufen. Der Ablaufsteuerungsschutz bietet eine wichtige zusätzliche Schutzebene für Device Guard. Wenn eine aufgeführte Anwendung kompromittiert wurde, kann Sie von Device Guard nicht überprüft werden, da das Device Guard-Screening sehen würde, dass die Anwendung signiert wurde und als vertrauenswürdig eingestuft wird.

Da der Ablaufsteuerungsschutz jedoch erkennen kann, ob die Anwendung in einer nicht vordefinierten, nicht ordnungsgemäß ausgeführten Reihenfolge ausgeführt wird, würde der Angriff fehlschlagen, wodurch verhindert wird, dass die kompromittierte Anwendung ausgeführt wird. Diese Schutzmaßnahmen erleichtern Angreifern das Einfügen von Schadsoftware in Software, die unter Windows Server 2016 ausgeführt wird.

Entwickler, die Anwendungen entwickeln, in denen persönliche Daten verarbeitet werden, werden empfohlen, den Ablaufsteuerungsschutz (Control Flow Guard, CFG) in Ihren Anwendungen zu aktivieren. Diese Funktion ist in Microsoft Visual Studio 2015 verfügbar und wird unter "CFG-fähige" Versionen von Windows – den x86- und x64-Releases für Desktop und Server von Windows 10 und Windows 8.1 Update (KB3000850) ausgeführt. Sie müssen CFG nicht für jeden Teil Ihres Codes aktivieren, da eine Mischung aus CFG-aktiviertem und nicht CFG-aktiviertem Code problemlos ausgeführt werden kann. Wenn aber CFG nicht für den gesamten Code aktiviert werden kann, können Lücken im Schutz geöffnet werden. Außerdem funktioniert der CFG-aktivierte Code in den "CFG-nicht"-Versionen von Windows einwandfrei und ist daher vollständig kompatibel mit diesen.

Windows Defender Antivirus

Windows Server 2016 umfasst die branchenführenden, aktiven Erkennungsfunktionen von Windows Defender zum Blockieren bekannter Schadsoftware. Windows Defender Antivirus (AV) kann zusammen mit Windows Defender Device Guard und Ablaufsteuerungsschutz verwendet werden, um zu verhindern, dass bösartiger Code jeglicher Art auf Ihren Servern installiert wird. Diese Einstellung ist standardmäßig aktiviert – der Administrator muss keine Maßnahmen ergreifen, um mit der Arbeit zu beginnen. Windows Defender AV ist auch für die Unterstützung der verschiedenen Serverrollen in Windows Server 2016 optimiert. In der Vergangenheit nutzten die Angreifer Shells wie z. B. PowerShell, um bösartigen Binärcode zu starten. In Windows Server 2016 ist PowerShell nun in Windows Defender AV integriert, um vor dem Starten des Codes Schadsoftware zu überprüfen.

Windows Defender AV ist eine integrierte Antischadsoftwarelösung, die die Verwaltung von Sicherheits- und Antischadsoftware für Desktops, tragbare Computer und Server ermöglicht. Windows Defender AV wurde seit der Einführung in Windows 8 erheblich verbessert. Windows Defender Antivirus in Windows Server verwendet einen mehrstufigen Ansatz, um Antischadsoftware zu verbessern:

- **Von der Cloud bereitgestellter Schutz** erkennt und blockiert neue Schadsoftware innerhalb von Sekunden, auch wenn die Schadsoftware bisher noch nie vorgekommen ist.
- **Umfassender lokaler Kontext** verbessert die Identifizierung von Schadsoftware. Windows Server informiert Windows Defender AV nicht nur über Inhalte wie Dateien und Prozesse, sondern auch über den Speicherort der Inhalte, wo Sie gespeichert wurden und vieles mehr.
- **Umfassende globale Sensoren** helfen dabei, Windows Defender AV auf dem neuesten Stand zu halten und selbst die neuesten Schadsoftware zu berücksichtigen. Dies erfolgt auf zwei Arten: durch Sammeln der Daten des umfassenden lokalen Kontexts von Endpunkten und das zentrale Analysieren dieser Daten.
- **Manipulationsschutz** schützt Windows Defender AV selbst gegen Angriffe durch Schadsoftware. Beispielsweise verwendet Windows Defender AV geschützte Prozesse, wodurch verhindert wird, dass nicht vertrauenswürdige Prozesse versuchen, Windows Defender AV-Komponenten, deren Registrierungsschlüssel usw. zu manipulieren.
- **Features auf Unternehmensebene** ermöglichen IT-Experten die Tools und Konfigurationsoptionen, die erforderlich sind, um Windows Defender AV zu einer Lösung für die Unternehmens-Antischadsoftware zu machen.

Verstärkte Sicherheitsüberwachung

Windows Server 2016 warnt Administratoren aktiv durch die verstärkte Sicherheitsüberprüfung, die ausführlichere Informationen bereitstellt, die zur schnelleren Erkennung von Angriffen und forensischen Analysen verwendet werden können. Es protokolliert Ereignisse von Ablauf Steuerungs Schutz, Windows Defender Device Guard und anderen Sicherheitsfeatures an einem Ort, sodass Administratoren leichter feststellen können, welche Systeme gefährdet sind.

Zu den neuen Ereignis Kategorien gehören:

- **Überwachen der Gruppenmitgliedschaft.** Ermöglicht es Ihnen, die Gruppen Mitgliedschafts Informationen im Anmelde Token eines Benutzers zu überwachen. Ereignisse werden generiert, wenn Gruppenmitgliedschaften auf dem PC aufgelistet oder abgefragt werden, auf dem die Anmelde Sitzung erstellt wurde.
- **Überwachen der PNP-Aktivität.** Ermöglicht Ihnen, zu überwachen, wann Plug & Play ein externes Gerät erkennt – das möglicherweise Schadsoftware enthält. PNP-Ereignisse können verwendet werden, um Änderungen an der System Hardware zu verfolgen. Im Ereignis ist eine Liste der Hardwarehersteller-IDs enthalten.

Windows Server 2016 lässt sich problemlos mit den SIEM-Systemen (Security Incident Management), wie z. b. Microsoft Operations Management Suite (OMS), integrieren, die die Informationen zu potenziellen Sicherheitsverletzungen in Intelligence-Berichte integrieren können. Die Tiefe der von der erweiterten Überwachung bereitgestellten Informationen ermöglicht es Sicherheitsteams, potenzielle Verletzungen schneller und effektiver zu erkennen und darauf zu reagieren.

Sichere Virtualisierung

Unternehmen virtualisieren heute alles, was Sie können, von SQL Server zu SharePoint auf Active Directory-Domäne Controller. Virtuelle Computer (Virtual Machines, VMS) vereinfachen die Bereitstellung, Verwaltung, Verwaltung und Automatisierung Ihrer Infrastruktur. Wenn es jedoch um die Sicherheit geht, werden gefährdete virtualisierungsfabrics zu einem neuen Angriffsvektor, der schwer gegen – schwer zu verteidigen ist. Aus Gründen der dsgvo sollten Sie sich Gedanken über den Schutz von VMS machen, wenn Sie physische Server schützen, einschließlich der Verwendung der VM-TPM-Technologie.

Windows Server 2016 ändert grundlegend, wie Unternehmen die Virtualisierung sichern können, indem Sie mehrere Technologien einschließen, die es Ihnen ermöglichen, virtuelle Maschinen zu erstellen, die nur in Ihrem eigenen Fabric ausgeführt werden. Schutz vor der Speicherung, dem Netzwerk und den Host Geräten, auf denen Sie ausgeführt werden.

Abgeschirmte virtuelle Computer

Die gleichen Dinge, die virtuelle Computer so einfach zu migrieren, zu sichern und zu replizieren, erleichtern das ändern und Kopieren von Daten. Bei einem virtuellen Computer handelt es sich lediglich um eine Datei, sodass er nicht im Netzwerk, im Speicher, in Sicherungen oder an anderen Orten geschützt ist. Ein weiteres Problem ist, dass fabricadministratoren – ob es sich um einen Speicher Administrator oder einen Netzwerkadministrator handelt – Zugriff auf alle virtuellen Computer haben.

Ein kompromittierter Administrator im Fabric kann problemlos zu kompromittierten Daten auf virtuellen Computern führen. Alle Angreifer müssen die kompromittierten Anmelde Informationen verwenden, um beliebige VM-Dateien auf ein USB-Laufwerk zu kopieren und diese aus der Organisation zu kopieren, in der von jedem anderen System aus auf diese VM-Dateien zugegriffen werden kann. Wenn einer dieser gestohlenen VMS ein Active Directory Domänen Controller wäre, könnte der Angreifer den Inhalt problemlos anzeigen und sofort verfügbare Brute-Force-Techniken verwenden, um die Kenn Wörter in der Active Directory Datenbank zu knacken und Ihnen schließlich Zugriff zu gewähren. für alle anderen Elemente in Ihrer Infrastruktur.

Windows Server 2016 führt abgeschirmte Virtual Machines (abgeschirmte VMS) ein, um den Schutz vor Szenarien wie dem soeben beschriebenen Szenario zu erleichtern. Abgeschirmte VMS enthalten ein virtuelles TPM-Gerät, mit

dem Organisationen die BitLocker-Verschlüsselung auf die virtuellen Computer anwenden und sicherstellen können, dass Sie nur auf vertrauenswürdigen Hosts ausgeführt werden, um Schutz vor gefährdeten Speicher-, Netzwerk- und Host Administratoren zu bieten. Abgeschirmte VMS werden mithilfe von VMS der Generation 2 erstellt, die Unified Extensible Firmware Interface-Firmware (UEFI) unterstützen und über ein virtuelles TPM verfügen.

Host-Überwachungsdienst

Neben abgeschirmten VMS ist der Host-Überwachungsdienst eine wesentliche Komponente zum Erstellen eines sicheren virtualisierungsfabrics. Seine Aufgabe besteht darin, die Integrität eines Hyper-V-Hosts zu bestätigen, bevor eine abgeschirmte VM gestartet oder zu diesem Host migriert werden kann. Sie enthält die Schlüssel für abgeschirmte VMS und gibt Sie erst frei, wenn die Sicherheits Integrität gewährleistet ist. Es gibt zwei Möglichkeiten, wie Sie Hyper-V-Hosts zum Bestätigen des Host-Überwachungs Diensts auffordern können.

Der erste und sicherste Nachweis ist der Hardware vertrauenswürdige Nachweis. Diese Lösung erfordert, dass Ihre abgeschirmten VMS auf Hosts mit TPM 2,0-Chips und UEFI 2.3.1 ausgeführt werden. Diese Hardware ist erforderlich, um die vom Host-Überwachungsdienst benötigten Informationen zur Start- und Betriebssystem-Kernel Integrität bereitzustellen, um sicherzustellen, dass der Hyper-V-Host nicht manipuliert wurde.

IT-Organisationen haben eine Alternative zur Verwendung von Administrator vertrauenswürdigen Nachweis. Dies ist möglicherweise wünschenswert, wenn die TPM 2,0-Hardware in Ihrer Organisation nicht verwendet wird. Dieses Nachweis Modell ist einfach bereitzustellen, weil Hosts einfach in eine Sicherheitsgruppe eingefügt werden und der Host-Überwachungsdienst so konfiguriert ist, dass abgeschirmte VMS auf Hosts ausgeführt werden können, die Mitglieder der Sicherheitsgruppe sind. Bei dieser Methode gibt es keine komplexe Messung, um sicherzustellen, dass der Host Computer nicht manipuliert wurde. Allerdings ist es nicht möglich, dass unverschlüsselte VMS auf USB-Laufwerken die Tür durchlaufen oder dass die VM auf einem nicht autorisierten Host ausgeführt wird. Dies liegt daran, dass die VM-Dateien nicht auf Computern ausgeführt werden, die nicht in der angegebenen Gruppe vorhanden sind. Wenn Sie noch nicht über TPM 2,0-Hardware verfügen, können Sie mit dem Administrator vertrauenswürdigen Nachweis beginnen und zum Hardware vertrauenswürdigen Nachweis wechseln, wenn die Hardware aktualisiert wird.

Virtueller Computer Trusted Platform Module

Windows Server 2016 unterstützt TPM für virtuelle Computer, sodass Sie erweiterte Sicherheitstechnologien wie BitLocker® Laufwerk Verschlüsselung auf virtuellen Computern unterstützen können. Sie können die TPM-Unterstützung auf jedem virtuellen Hyper-v-Computer der Generation 2 mithilfe des Hyper-v-Managers oder des Windows PowerShell-Cmdlets Enable-vmtpm aktivieren.

Sie können das virtuelle TPM (vtpm) schützen, indem Sie die lokalen Kryptografieschlüssel verwenden, die auf dem Host gespeichert oder im Host-Überwachungsdienst gespeichert sind. Obwohl der Host-Überwachungsdienst mehr Infrastruktur benötigt, bietet er auch mehr Schutz.

Verteilte Netzwerk Firewall mit Software-Defined Networking

Eine Möglichkeit, den Schutz in virtualisierten Umgebungen zu verbessern, besteht darin, das Netzwerk so zu segmentieren, dass es VMS nur mit den spezifischen Systemen kommunizieren kann, die für die Funktion erforderlich sind. Wenn Ihre Anwendung z. B. keine Verbindung mit dem Internet herstellen muss, können Sie Sie partitionieren, sodass diese Systeme als Ziele von externen Angreifern entfernt werden. Das Software-Defined Networking (SDN) in Windows Server 2016 umfasst eine verteilte Netzwerk Firewall, die es Ihnen ermöglicht, die Sicherheitsrichtlinien, mit denen Ihre Anwendungen vor Angriffen innerhalb oder außerhalb eines Netzwerks geschützt werden können, dynamisch zu erstellen. Diese verteilte Netzwerk Firewall fügt Ihrer Sicherheit Ebenen hinzu, indem Sie Ihre Anwendungen im Netzwerk isolieren können. Richtlinien können überall in Ihrer virtuellen Netzwerkinfrastruktur angewendet werden, wobei der VM-zu-VM-Datenverkehr, der VM-zu-Host-Datenverkehr oder der VM-zu-Internet-Datenverkehr bei Bedarf isoliert wird – entweder für einzelne Systeme, die möglicherweise kompromittiert oder Programm gesteuert über mehrere Subnetze. Mit den Software definierten Netzwerkfunktionen von Windows Server 2016 können Sie eingehenden Datenverkehr auch an virtuelle Geräte außerhalb von Microsoft weiterleiten oder spiegeln. Beispielsweise können Sie den gesamten e-Mail-Datenverkehr über ein virtuelles Barracuda-Gerät senden, um zusätzlichen Schutz vor Spam Filtern zu erhalten. Dies ermöglicht

es Ihnen, auf einfache Weise zusätzliche Sicherheit sowohl lokal als auch in der Cloud zu ermöglichen.

Weitere ds-gvo-Überlegungen zu Servern

Die ds-gvo beinhaltet explizite Anforderungen für Verstöße gegen Benachrichtigungen, bei denen eine persönliche Datenverletzung bedeutet: *"eine Sicherheitsverletzung, die zur versehentlichen oder ungesetzlichen Zerstörung, Verlust, Änderung, nicht autorisierter Offenlegung oder Zugriff auf, übermittelte oder anderweitig verarbeitete personenbezogene Daten führt."* Natürlich können Sie nicht fortfahren, um die strengen Anforderungen an die ds-gvo-Benachrichtigung innerhalb von 72 Stunden zu erfüllen, wenn Sie die Sicherheitslücke überhaupt nicht erkennen können.

Wie im Windows-Security Center Whitepaper zu beachten, stellen Sie die [nach Verletzung: Umgang mit erweiterten Bedrohungen](#)

"Anders als bei der vor- und nach Verletzung geht die nach Verletzung davon aus, dass bereits eine Verletzung aufgetreten ist – fungiert als Flight Recorder und Crime Scene Investigator (CSI). Die nach Verletzung bietet Sicherheitsteams die erforderlichen Informationen und Toolsets, um Angriffe zu identifizieren, zu untersuchen und darauf zu reagieren, die andernfalls nicht erkannt werden und sich unter dem Netz befinden."

In diesem Abschnitt erfahren Sie, wie Sie mithilfe von Windows Server Ihre ds-gvo-Benachrichtigungs Verpflichtungen erfüllen können. Dies beginnt mit dem Verständnis der zugrunde liegenden Bedrohungs Daten, die Microsoft zur Verfügung steht und die für Ihren Vorteil gesammelt und analysiert werden, und wie Sie über Windows Defender Advanced Threat Protection (ATP) für Sie von entscheidender Bedeutung sein können.

Aufschlussreiche Sicherheitsdiagnosedaten

Seit fast zwei Jahrzehnten hat Microsoft Bedrohungen in nützliche Informationen verwandelt, mit denen die Plattform und der Schutz von Kunden unterstützt werden können. Dank der großen Computing-Vorteile von heute durch die Cloud, finden wir neue Verwendungsmöglichkeiten für unsere umfangreiche Analysemodule, die von der Bedrohungserkennung verursacht und zum Schutz unserer Kunden sind.

Durch das Anwenden einer Kombination von automatisierten und manuellen Prozessen, Machine Learning und menschlichen Experten, können wir ein intelligentes Security-Diagramm erstellen, das von sich selbst lernt und sich in Echtzeit weiter entwickelt, um neue Bedrohungen für unsere Produkte zu erkennen und darauf zu reagieren.



Der Umfang der Bedrohungs Intelligenz von Microsoft umfasst im wesentlichen Milliarden von Datenpunkten: 35 Milliarden Nachrichten monatlich, 1 Milliarde Kunden in Unternehmens- und consumersegmenten, die auf 200 + Cloud-Dienste und 14 Milliarden Authentifizierungen ausgeführt werden. tä. Alle diese Daten werden in Ihrem

Auftrag von Microsoft zusammengeführt, um die intelligent Security Graph zu erstellen, die Ihnen helfen, Ihre Front-Door-Sicherheit auf dynamische Weise zu schützen, weiterhin produktiv zu bleiben und die Anforderungen der DSGVO zu erfüllen.

Erkennen von Angriffen und forensische Untersuchung

Auch die besten Endpoint-Schutzmaßnahmen können irgendwann überwunden werden, da Cyberangriffe mehr ausgefeilt und zielgerichtet sind. Zwei Funktionen können zur Unterstützung der Erkennung möglicher Sicherheitsverletzungen verwendet werden: Windows Defender Advanced Threat Protection (ATP) und Microsoft Advanced Threat Analytics (ATA).

Windows Defender Advanced Threat Protection (ATP) hilft Ihnen, fortgeschrittene Angriffe zu erkennen und untersuchen und auf Datenschutzverletzungen im Netzwerk zu reagieren. Die Typen der Datenverletzung, die für die DSGVO durch technische Sicherheitsmaßnahmen geschützt werden müssen, um die fortlaufende Vertraulichkeit, Integrität und Verfügbarkeit von persönlichen Daten und Verarbeitungssystemen sicherzustellen.

Zu den wichtigsten Vorteilen von Windows Defender ATP zählen die folgenden:

- **Erkennen der nicht erkennbaren.** Sensoren, die tief in den Kernel des Betriebssystems, Windows-Sicherheitsexperten und eindeutige Optiken integriert sind, von über 1 Milliarde Computern und Signalen über alle Microsoft-Dienste hinweg.
- **Integriert, nicht fett formatiert.** Ohne Agent, mit hoher Leistung und minimaler Auswirkung, cloudbasiert; einfache Verwaltung ohne Bereitstellung.
- **Einzelner Glasbereich für Windows-Sicherheit.** Erkunden Sie den umfangreichen Zeitraum von 6 Monaten, Machine-Timeline und Vereinheitlichung von Sicherheits Ereignissen von Windows Defender ATP, Windows Defender Antivirus und Windows Defender Device Guard.
- **Leistungsfähigkeit von Microsoft Graph.** Nutzt das Microsoft Intelligence Security Graph, um die Erkennung und Untersuchung mit dem Office 365 ATP-Abonnement zu integrieren, um Angriffe zurückverfolgen und darauf reagieren zu können.

Weitere Informationen finden Sie unter Neuigkeiten [in der Windows Defender ATP Creators Update-Vorschau](#).

ATA ist ein lokales Produkt, mit dem Identitäts Gefährdung in einer Organisation erkannt werden kann. ATA kann Netzwerk Datenverkehr für Authentifizierungs-, Autorisierungs- und Informations Sammel Protokolle (z. B. Kerberos, DNS, RPC, NTLM und andere Protokolle) erfassen und analysieren. ATA verwendet diese Daten, um ein Verhaltensprofil für Benutzer und andere Entitäten in einem Netzwerk zu erstellen, damit Anomalien und bekannte Angriffsmuster erkannt werden können. In der folgenden Tabelle sind die von ATA erkannten Angriffstypen aufgeführt.

ANGREITERTYP	BESCHREIBUNG
Böswillige Angriffe	<p>Diese Angriffe werden erkannt, indem Sie nach Angriffen aus einer bekannten Liste von Angriffstypen suchen, einschließlich:</p> <ul style="list-style-type: none">• Pass-the-Ticket (PtT)• Pass-the-Hash (PtH)• Overpass-the-Hash• Forged PAC (MS14-068)• Golden Ticket• Böswillige Replikationen• Erkundung• Brute-Force-Angriffe• Remoteausführung <p>Eine umfassende Liste der gefundenen böswilligen Angriffe und deren Beschreibung finden Sie unter welche verdächtigen Aktivitäten können von ATA erkannt werden?</p>

ANGREITERTYP	BESCHREIBUNG
Ungewöhnliches Verhalten	<p>Diese Angriffe werden mithilfe der Verhaltensanalyse erkannt und verwenden Machine Learning, um fragwürdige Aktivitäten zu identifizieren, einschließlich:</p> <ul style="list-style-type: none"> • Nicht normale Anmeldungen • Unbekannte Gefahren • Kennwortfreigabe • "Seitwärtsbewegung"
Sicherheitsprobleme und-Risiken	<p>Diese Angriffe werden erkannt, wenn Sie die aktuelle Netzwerk- und Systemkonfiguration betrachten, einschließlich:</p> <ul style="list-style-type: none"> • einer fehlerhaften Vertrauensstellung • schwacher Protokolle • bekannter Protokollschwachstellen.

Mithilfe von ATA können Sie Angreifer erkennen, die versuchen, privilegierte Identitäten zu kompromittieren. Weitere Informationen zum Bereitstellen von ATA finden Sie in den Themen Plan, Entwurf und Bereitstellung in der [Advanced Threat Analytics-Dokumentation](#).

Verwandte Inhalte für zugehörige Windows Server 2016-Lösungen

- **Windows Defender Antivirus:** <https://www.youtube.com/watch?v=P1aNEy09NaI> und <https://docs.microsoft.com/windows/threat-protection/windows-defender-antivirus/windows-defender-antivirus-in-windows-10>
- **Windows Defender Advanced Threat Protection:** <https://www.youtube.com/watch?v=qxeGa3pxlwg> und <https://docs.microsoft.com/windows/threat-protection/windows-defender-atp/configure-server-endpoints-windows-defender-advanced-threat-protection>
- **Windows Defender Device Guard:** <https://www.youtube.com/watch?v=F-pTkesjkhI> und <https://docs.microsoft.com/windows/device-security/device-guard/device-guard-deployment-guide>
- **Windows Defender Credential Guard:** <https://www.youtube.com/watch?v=F-pTkesjkhI> und <https://docs.microsoft.com/windows/access-protection/credential-guard/credential-guard>
- **Ablauf Steuerungs Schutz:** [https://msdn.microsoft.com/library/windows/desktop/mt637065\(v=vs.85\).aspx](https://msdn.microsoft.com/library/windows/desktop/mt637065(v=vs.85).aspx)
- **Sicherheit und Sicherheit:** <https://docs.microsoft.com/windows-server/security/security-and-assurance>

Haftungsausschluss

Dieser Artikel enthält einen Kommentar über die GDPR wie Microsoft ihn ab dem Datum der Veröffentlichung interpretiert. Wir haben viel Zeit mit dsgvo verbracht und wissen, dass wir uns Gedanken über seine Absicht und Bedeutung gemacht haben. Die Anwendung der GDPR ist jedoch äußerst tatsächenspezifisch, und die Aspekte und Interpretationen der GDPR sind nicht definitiv beigelegt.

Daher dient dieser Artikel nur zu Informationszwecken und sollte nicht zuverlässig als rechtlicher Hinweise angesehen werden oder um zu bestimmen, wie die GDPR für Sie und Ihr Unternehmen angewendet wird. Wir empfehlen Ihnen, die mit einem gesetzlich qualifizierten Experten zusammen zu arbeiten, um die GDPR zu besprechen, wie sie speziell für Ihre Organisation angewendet wird und wie sie am besten funktioniert, um Kompatibilität zu gewährleisten.

MICROSOFT GIBT IN BEZUG AUF DIE INFORMATIONEN IN DIESEM ARTIKEL KEINERLEI GEWÄHRLEISTUNG, WEDER AUSDRÜCKLICH NOCH KONKLUDENT. Dieser Artikel wird auf "as-is"-Basis bereitgestellt. Die in diesem Artikel

gegebenen Informationen und Ansichten, darunter URLs und andere Verweise auf Internetseiten, können ohne vorherige Ankündigung geändert werden.

Dieser Artikel stellt Ihnen keinerlei Rechte am geistigen Eigentum eines beliebigen Microsoft-Produkts zur Verfügung. Dieser Artikel darf nur für interne Zwecke kopiert und verwendet werden.

Veröffentlicht: September 2017

Version 1.0

© 2017 Microsoft. Alle Rechte vorbehalten.

Geschütztes Fabric und abgeschirmte VMs

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Eines der wichtigsten Ziele bei der Bereitstellung einer gehosteten Umgebung besteht darin, die Sicherheit der virtuellen Computer zu gewährleisten, die in der Umgebung ausgeführt werden. Als Cloud-Dienstanbieter oder privater Cloud-Administrator im Unternehmen können Sie ein geschütztes Fabric verwenden, um eine sicherere Umgebung für VMs bereitzustellen. Ein geschütztes Fabric besteht aus einem Host Guardian Service (Host-Überwachungsdienst) – in der Regel ein Cluster mit drei Knoten – sowie einem oder mehreren geschützten Hosts und einer Reihe von abgeschirmten virtuellen Computern (VMs).

IMPORTANT

Stellen Sie sicher, dass Sie das neueste kumulative Update installiert haben, bevor Sie geschützte virtuelle Computer in der Produktion bereitstellen.

Videos, Blog und Übersichts Thema zu geschützten Fabrics und abgeschirmten VMS

- Video: [Schützen Ihres virtualisierungsfabrics vor Insider Bedrohungen mit Windows Server 2019](#)
- Video: [Einführung in abgeschirmte Virtual Machines in Windows Server 2016](#)
- Video: [Einblicke in abgeschirmte VMS mit Windows Server 2016 Hyper-V](#)
- Video: [bereitstellen von abgeschirmten VMS und einem geschützten Fabric mit Windows Server 2016](#)
- Blog: [Daten Center-und Private Cloud-Sicherheitsblog](#)
- Übersicht: [Übersicht über geschützte Fabric-und abgeschirmte VMS](#)

Themen zur Planung

- [Planungs Handbuch für Hoster](#)
- [Planungs Handbuch für Mandanten](#)

Themen zur Bereitstellung

- [Bereitstellungs Handbuch](#)
 - [Schnellstart](#)
 - [Bereitstellen von HGS](#)
 - [Bereitstellen geschützter Hosts](#)
 - [Konfigurieren des Fabric-DNS für Hosts, die zu überwachten Hosts werden](#)
 - [Bereitstellen eines überwachten Hosts im AD-Modus](#)
 - [Bereitstellen eines überwachten Hosts mit dem TPM-Modus](#)
 - [Bestätigen, dass geschützte Hosts bestätigen können](#)
 - [Abgeschirmte VMS: der hostingdienstanbieter stellt überwachte Hosts in VMM bereit.](#)
 - [Bereitstellen von abgeschirmten VMs](#)
 - [Erstellen einer abgeschirmten VM-Vorlage](#)
 - [Vorbereiten einer VHD für ein VM-Schutz Hilfsprogramm](#)

- Einrichten des Windows Azure Packs
- Erstellen einer Schutz Datendatei
- Bereitstellen einer abgeschirmten VM mithilfe Windows Azure Pack
- Bereitstellen einer abgeschirmten VM mithilfe Virtual Machine Manager

Themen zur Betriebs-und Verwaltungsaufgaben

- Verwalten des Host-Überwachungs Diensts

Übersicht über geschütztes Fabric und abgeschirmte VMs

09.04.2020 • 24 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Übersicht zu geschütztem Fabric

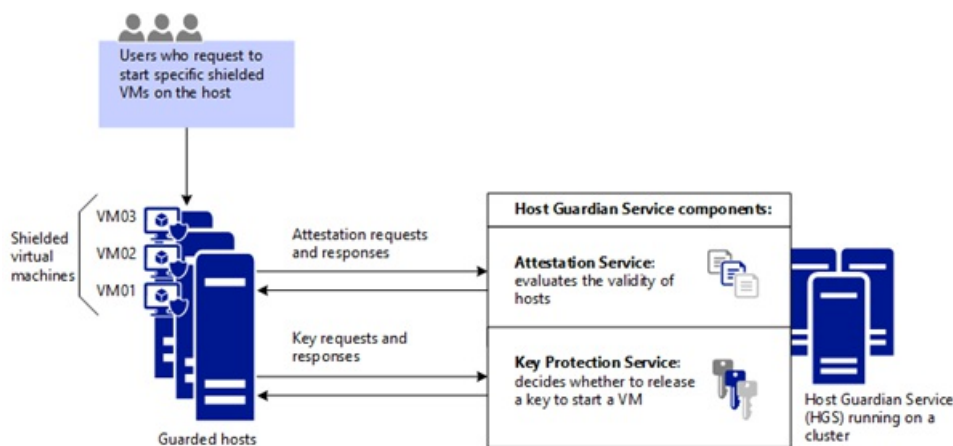
Virtualisierungssicherheit ist ein wichtiger Investitionsbereich in Hyper-V. Zusätzlich zum Schutz von Hosts oder anderen virtuellen Computern vor einem virtuellen Computer mit Malware müssen wir virtuelle Computer auch vor einem gefährdeten Host schützen. Dies ist eine grundlegende Gefahr für jede Virtualisierungsplattform, egal ob Hyper-V, VMware oder eine andere Virtualisierungsplattform. Ganz einfach – wenn ein virtueller Computer aus einer Organisation herausgenommen wird (in böswilliger Absicht oder versehentlich), kann diese VM auf jedem anderen System ausgeführt werden. Der Schutz wertvoller Ressourcen in Ihrer Organisation, z.B. Domänencontroller, vertrauliche Dateiserver und Personalverwaltungssysteme, hat oberste Priorität.

Zur Unterstützung des Schutzes vor kompromittiertem virtualisierungsfabric führte Windows Server 2016 Hyper-V abgeschirmte VMS ein. Eine abgeschirmte VM ist eine VM der Generation 2 (unterstützt unter Windows Server 2012 und höher), die über ein virtuelles TPM verfügt, mit BitLocker verschlüsselt ist und nur auf fehlerfreien und genehmigten Hosts im Fabric ausgeführt werden kann. Abgeschirmte VMs und geschütztes Fabric ermöglichen Clouddiensteanbietern oder Private Cloud-Administratoren in Unternehmen, eine sichere Umgebung für Mandanten-VMs bereitzustellen.

Ein geschütztes Fabric besteht aus:

- 1 Host-Überwachungsdienst (Host Guardian Service, HGS) (in der Regel ein Cluster mit 3 Knoten)
- Mindestens ein geschützter Host
- Eine Gruppe abgeschirmter virtueller Computer. Das folgende Diagramm zeigt, wie der Host-Überwachungsdienst den Nachweis verwendet, um sicherzustellen, dass nur bekannte und gültige Hosts die abgeschirmte VM starten können, und den Schlüsselschutzdienst, um die Schlüssel für abgeschirmte VMs sicher freizugeben.

Wenn ein Mandant abgeschirmte VMs erstellt, die auf einem geschützten Fabric ausgeführt werden, werden die Hyper-V-Hosts und die abgeschirmten VMs selbst durch den Host-Überwachungsdienst geschützt. Der Host-Überwachungsdienst bietet zwei verschiedene Dienste: Nachweis und Schlüsselschutz. Der Nachweisdienst stellt sicher, dass nur vertrauenswürdige Hyper-V-Hosts abgeschirmte VMs ausführen können, während der Schlüsselschutzdienst die Schlüssel bereitstellt, die erforderlich sind, um sie einzuschalten und ihre Livemigration zu anderen geschützten Hosts durchzuführen.



Video: Einführung in abgeschirmte virtuelle Maschinen

<https://channel9.msdn.com/Shows/Mechanics/Introduction-to-Shielded-Virtual-Machines-in-Windows-Server-2016/player>

Nachweismodi in der „Geschütztes Fabric“-Lösung

Die HGS unterstützen verschiedene Nachweis Modi für ein geschütztes Fabric:

- TPM-vertrauenswürdiger Nachweis (Hardware basiert)
- Host Schlüssel Nachweis (basierend auf asymmetrischen Schlüsselpaaren)

Der TPM-vertrauenswürdige Nachweis wird empfohlen, da er stärkere Garantien bietet, wie in der folgenden Tabelle beschrieben, setzt aber voraus, dass Ihre Hyper-V-Hosts über TPM 2.0 verfügen. Wenn Sie derzeit nicht über TPM 2,0 oder ein TPM verfügen, können Sie den Host Schlüssel Nachweis verwenden. Wenn Sie sich für den Wechsel zum TPM-vertrauenswürdigen Nachweis entscheiden, wenn Sie neue Hardware erwerben, können Sie den Nachweismodus auf dem Host-Überwachungsdienst mit minimaler oder ohne Unterbrechung Ihres Fabric's wechseln.

NACHWEIS MODUS, DEN SIE FÜR HOSTS AUSWÄHLEN	HOST ZUSICHERUNGEN
TPM-vertrauenswürdiger Nachweis: bietet den stärksten Schutz, erfordert jedoch auch weitere Konfigurationsschritte. Host Hardware und Firmware müssen TPM 2,0 und UEFI 2.3.1 mit aktiviertem sicheren Start einschließen.	Geschützte Hosts werden basierend auf der TPM-Identität, der gemessenen Startsequenz und den Code Integritäts Richtlinien genehmigt, um sicherzustellen, dass Sie nur genehmigten Code ausführen.
Host Schlüssel Nachweis: Dient zur Unterstützung vorhandener Host Hardware, bei der TPM 2,0 nicht verfügbar ist. Erfordert weniger Konfigurationsschritte und ist kompatibel mit gängiger Serverhardware.	Geschützte Hosts werden basierend auf dem Besitz des Schlüssels genehmigt.

Ein anderer Modus mit dem Namen **Admin-Trusted Nachweis** ist ab Windows Server 2019 veraltet. Dieser Modus basiert auf der überwachten Host Mitgliedschaft in einer festgelegten Active Directory Domain Services (AD DS)-Sicherheitsgruppe. Der Host Schlüssel Nachweis bietet eine ähnliche Host Identifizierung und ist leichter einzurichten.

Garantien, die der Host-Überwachungsdienst bietet

Der Host-Überwachungsdienst bietet zusammen mit den Methoden zum Erstellen abgeschirmter VMs die folgenden Garantien.

ART DER SICHERUNG FÜR VMS	GESCHÜTZTE VM-ZUSICHERUNGEN, VOM SCHLÜSSELSCHUTZ DIENST UND VON ERSTELLUNGS METHODEN FÜR ABGESCHIRMTE VMS
BitLocker-verschlüsselte Datenträger (Betriebssystem-Datenträger und Datenträger)	<p>Abgeschirmte VMs verwenden BitLocker zum Schutz ihrer Datenträger. Die BitLocker-Schlüssel, die zum Starten des virtuellen Computers und zum Entschlüsseln der Datenträger erforderlich sind, werden vom virtuellen TPM der abgeschirmten VM mithilfe von branchenspezifischen Technologien wie dem sicheren gemessenen Start geschützt. Während abgeschirmte VMs den Betriebssystemdatenträger nur automatisch verschlüsseln und schützen, können Sie der abgeschirmten VM angefügte Datenlaufwerke gleichermaßen verschlüsseln.</p>
Bereitstellung neuer abgeschirmter VMS aus "vertrauenswürdigen" Vorlagen Datenträgern/Images	<p>Bei der Bereitstellung neuer abgeschirmter VMs können Mandanten angeben, welche Vorlagedatenträger sie als vertrauenswürdige einstufen. Abgeschirmte Vorlagedatenträger verfügen über Signaturen, die zu einem Zeitpunkt berechnet werden, wenn ihre Inhalte als vertrauenswürdige eingestuft werden. Die Datenträgersignaturen werden dann in einem Signaturenkatalog gespeichert, den Mandanten beim Erstellen von abgeschirmten VMs sicher dem Fabric bereitstellen. Während der Bereitstellung abgeschirmter VMs wird die Signatur des Datenträgers erneut berechnet und mit den vertrauenswürdigen Signaturen im Katalog verglichen. Wenn die Signaturen übereinstimmen, wird die abgeschirmte VM bereitgestellt. Wenn die Signaturen nicht übereinstimmen, gilt der abgeschirmte Vorlagedatenträger als nicht vertrauenswürdige, und bei der Bereitstellung tritt ein Fehler auf.</p>
Schutz von Kenn Wörtern und anderen Geheimnissen beim Erstellen einer abgeschirmten VM	<p>Beim Erstellen von VMS muss sichergestellt werden, dass die VM-Geheimnisse, wie z. B. die vertrauenswürdigen Datenträger Signaturen, RDP-Zertifikate und das Kennwort des lokalen Administrator Kontos der VM, nicht an das Fabric weitergegeben werden. Diese vertraulichen Informationen befinden sich in einer als geschützte Datendatei (PDK-Datei) bezeichneten verschlüsselten Datei, die von Mandantenschlüsseln geschützt und vom Mandanten in das Fabric hochgeladen wird. Beim Erstellen einer abgeschirmten VM wählt der Mandant die zu verwendenden geschützten Daten aus, wodurch diese Informationen sicher nur den vertrauenswürdigen Komponenten innerhalb des geschützten Fabrics zur Verfügung gestellt werden.</p>
Mandanten Kontrolle über den Standort, an dem die VM gestartet werden kann	<p>Zu den geschützten Daten zählt auch eine Liste der geschützten Fabrics, in denen eine bestimmte abgeschirmte VM ausgeführt werden darf. Dies ist z.B. in Fällen hilfreich, in denen eine abgeschirmte VM sich typischerweise in einer lokalen privaten Cloud befindet, jedoch möglicherweise zur Wiederherstellung im Notfall zu einer anderen (öffentlichen oder privaten) Cloud migriert werden muss. Die Zielfabric oder das Zielfabric muss abgeschirmte VMs unterstützen, und die abgeschirmte VM muss dem Fabric die Ausführung genehmigen.</p>

Was sind geschützte Daten, und warum sind sie notwendig?

Eine geschützte Datendatei (auch als Bereitstellungsdatendatei oder PDK-Datei bezeichnet) ist eine verschlüsselte

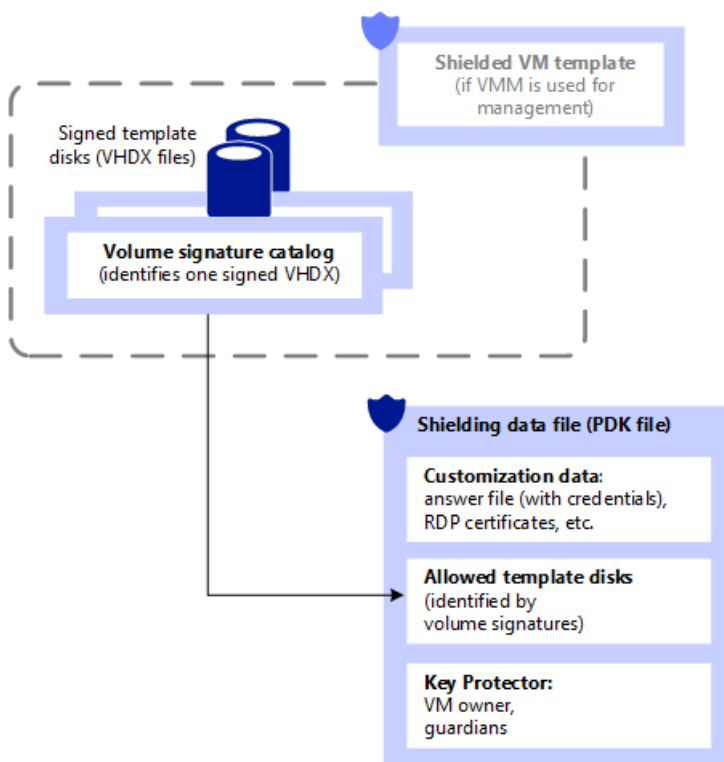
Datei, die ein Mandant oder VM-Besitzer erstellt, um wichtige VM-Konfigurationsinformationen, z.B. Administratorkennwort, RDP und andere identitätsbezogene Zertifikate, Domänenbeitritts-Anmeldeinformationen usw. zu schützen. Ein Fabricadministrator verwendet die geschützte Datendatei beim Erstellen einer abgeschirmten VM, kann die in der Datei enthaltenen Informationen allerdings nicht anzeigen oder verwenden.

Unter anderem enthalten geschützte Datendateien geheime Schlüssel wie z. B.:

- Administratoranmeldeinformationen
- Eine Antwortdatei („unattend.xml“)
- Eine Sicherheitsrichtlinie, die bestimmt, ob mit diesen Schutz Daten erstellte virtuelle Computer als abgeschirmt oder Verschlüsselung unterstützt werden.
 - Beachten Sie, dass als abgeschirmt konfigurierte VMs vor Fabricadministratoren geschützt sind, durch Verschlüsselung unterstützte VMs hingegen nicht.
- Ein RDP-Zertifikat zum Sichern der Remotedesktopkommunikation mit der VM
- Ein Volumesignaturkatalog, der eine Liste vertrauenswürdiger, signierter Vorlagedatenträger-Signaturen enthält, auf deren Basis eine neue VM erstellt werden kann
- Eine Schlüsselschutzvorrichtung (Key Protector, KP), die definiert, auf welchen geschützten Fabrics eine abgeschirmte VM ausgeführt werden darf

Die geschützte Datendatei (PDK) gewährleistet, dass die VM wie vom Mandanten vorgesehen erstellt wird. Wenn der Mandant z.B. eine Antwortdatei („unattend.xml“) in die geschützte Datendatei einfügt und sie an den Hostinganbieter übermittelt, kann der Hostinganbieter sie nicht anzeigen oder ändern. Ebenso kann der Hostinganbieter beim Erstellen der abgeschirmten VM keine andere VHDX verwenden, da die geschützte Datendatei die Signaturen des vertrauenswürdigen Datenträgers enthält, auf dessen Basis abgeschirmte VMs erstellt werden können.

Die folgende Abbildung zeigt die geschützte Datendatei und zugehörige Konfigurationselemente.



Welche Typen virtueller Computer kann ein geschütztes Fabric ausführen?

Geschützte Fabrics können VMs in einer von drei möglichen Arten ausführen:

1. Eine normale VM, die gegenüber früheren Versionen von Hyper-V weder mehr noch weniger Schutz bietet
2. Eine durch Verschlüsselung unterstützte VM, deren Schutzmaßnahmen durch einen Fabricadministrator konfiguriert werden können
3. Eine abgeschirmte VM, bei der alle Schutzmaßnahmen aktiviert sind und nicht durch einen Fabricadministrator deaktiviert werden können

Durch Verschlüsselung unterstützte VMs sollen dort eingesetzt werden, wo die Fabricadministratoren voll vertrauenswürdig sind. Beispielsweise könnte ein Unternehmen ein geschütztes Fabric bereitstellen, um sicherzustellen, dass VM-Datenträger zur Einhaltung von Vorschriften im Ruhezustand verschlüsselt werden. Fabricadministratoren können weiterhin komfortable Verwaltungsfunktionen wie VM-Konsolenverbindungen, PowerShell Direct und andere Tools zur täglichen Verwaltung und Problembehandlung verwenden.

Abgeschirmte virtuelle Computer dienen zur Verwendung in Fabrics, in denen Daten und Status des virtuellen Computers sowohl vor Fabricadministratoren als auch nicht vertrauenswürdiger Software, die möglicherweise auf den Hyper-V-Hosts ausgeführt wird, geschützt werden müssen. Abgeschirmte VMs würden z.B. nie eine VM-Konsolenverbindung zulassen, während ein Fabricadministrator diesen Schutz für durch Verschlüsselung unterstützte VMs aktivieren oder deaktivieren kann.

In der folgenden Tabelle werden die Unterschiede zwischen Verschlüsselung unterstütztem und abgeschirmten VMS zusammengefasst.

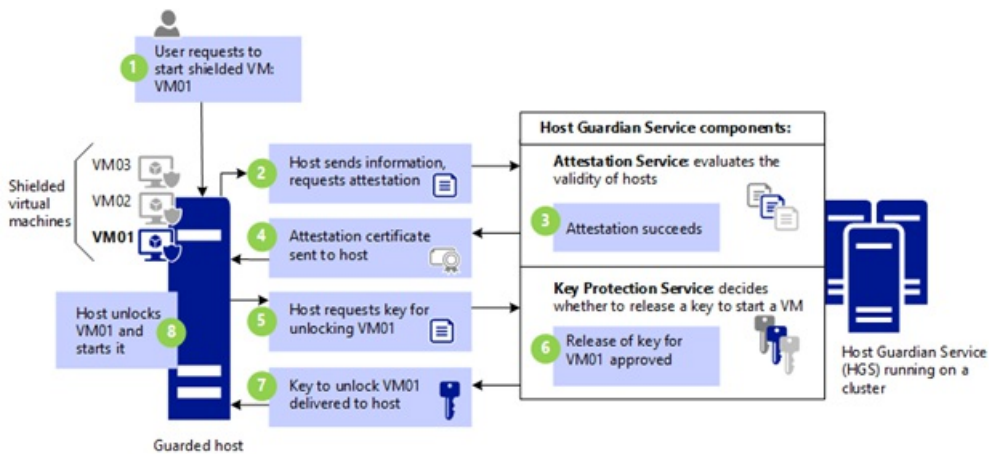
CAPABILITY	GENERATION 2 – DURCH VERSCHLÜSSELUNG UNTERSTÜTZT	GENERATION 2 – ABGESCHIRMT
Sicherer Start	Ja, erforderlich, aber konfigurierbar	Ja, erforderlich und erzwungen
Vtpm	Ja, erforderlich, aber konfigurierbar	Ja, erforderlich und erzwungen
Verschlüsseln des VM-Status und Livemigrations-Datenverkehr	Ja, erforderlich, aber konfigurierbar	Ja, erforderlich und erzwungen
Integrationskomponenten	Konfigurierbar durch Fabricadministrator	Bestimmte Integrationskomponenten blockiert (z.B. Datenaustausch, PowerShell Direct)
Verbindung mit virtuellen Computern (Konsole), HID-Geräte (z.B. Tastatur, Maus)	Ein, kann nicht deaktiviert werden	Aktiviert auf Hosts ab Windows Server-Version 1803; Auf früheren Hosts deaktiviert
COM/serielle Anschlüsse	Unterstützt	Deaktiviert (kann nicht aktiviert werden)
Anfügen eines Debuggers (an den VM-Prozess) ¹	Unterstützt	Deaktiviert (kann nicht aktiviert werden)

¹ herkömmliche Debugger, die direkt an einen Prozess angefügt werden (z. b. WinDbg.exe), werden für abgeschirmte VMS blockiert, da der Arbeitsprozess des virtuellen Computers (VMWP.exe) eine geschützte Prozess Beleuchtung (PPL) ist. Alternative Debuggingtechniken, z. b. die von LiveKd.exe verwendeten, werden nicht blockiert. Anders als bei abgeschirmten VMS wird der Arbeitsprozess für die Verschlüsselung unterstützte VMS nicht als ppl ausgeführt, sodass herkömmliche Debugger wie WinDBG.exe weiterhin normal funktionieren.

Sowohl abgeschirmte als auch durch Verschlüsselung unterstützte VMs unterstützen weiterhin gängige Fabricverwaltungsfunktionen wie Livemigration, Hyper-V-Replikate, VM-Prüfpunkt usw.

Der Host-Überwachungsdienst in Aktion: Wie ein abgeschirmter

virtuelle Computer eingeschaltet wird



1. VM01 ist eingeschaltet.

Bevor ein geschützter Host einen abgeschirmten virtuellen Computer einschalten kann, muss zuerst positiv nachgewiesen werden, dass er fehlerfrei ist. Um ihre Integrität nachzuweisen, muss sie dem Schlüsselschutzdienst (Key Protection Service, KPS) ein Integritätszertifikat vorlegen. Das Integritätszertifikat wird über den Nachweisprozess abgerufen.

2. Der Host fordert einen Nachweis an.

Der geschützte Host fordert einen Nachweis an. Der Nachweismodus wird durch den Host-Überwachungsdienst vorgegeben:

TPM-vertrauenswürdiger Nachweis: der Hyper-V-Host sendet Informationen, die Folgendes beinhalten:

```
- <span data-ttu-id="f37d1-229">TPM-identifizierende Informationen (seinen Endorsement Key)</span><span class="sxs-lookup"><span data-stu-id="f37d1-229">TPM-identifying information (its endorsement key)</span></span></span>
- <span data-ttu-id="f37d1-230">Informationen zu Prozessen, die während der letzten Startsequenz (TCG-Protokoll) gestartet wurden</span><span class="sxs-lookup"><span data-stu-id="f37d1-230">Information about processes that were started during the most recent boot sequence (the TCG log)</span></span>
- <span data-ttu-id="f37d1-231">Informationen zur Richtlinie für die Code Integrität (CI), die auf dem Host angewendet wurde.</span><span class="sxs-lookup"><span data-stu-id="f37d1-231">Information about the Code Integrity (CI) policy that was applied on the host.</span></span>
```

Attestation happens when the host starts and every 8 hours thereafter. If for some reason a host doesn't have an attestation certificate when a VM tries to start, this also triggers attestation.

Host Schlüssel Nachweis: der Hyper-V-Host sendet die öffentliche Hälfte des Schlüssel Paares. HGS überprüft, dass der Host Schlüssel registriert ist.

Admin-vertrauenswürdiger Nachweis: Hyper-V-Host sendet ein Kerberos-Ticket, das die Sicherheitsgruppen identifiziert, zu denen der Host gehört. Der Host-Überwachungsdienst überprüft, ob der Host zu einer Sicherheitsgruppe gehört, die zuvor vom vertrauenswürdigen HGS-Administrator konfiguriert wurde.

3. Nachweis erfolgreich (oder mit Fehler).

Der Nachweis Modus bestimmt, welche Überprüfungen erforderlich sind, um erfolgreich zu bestätigen, dass der Host fehlerfrei ist. Mit dem TPM-vertrauenswürdigen Nachweis werden die TPM-Identität des Hosts, Start Messungen und die Code Integritätsrichtlinie überprüft. Beim Nachweis des Host Schlüssels wird nur die Registrierung des Host Schlüssels überprüft.

4. Nachweiszertifikat wird an den Host gesendet.

Wenn der Nachweis erfolgreich war, wird ein Integritäts Zertifikat an den Host gesendet, und der Host wird als "geschützt" (autorisiert zum Ausführen von abgeschirmten VMS) betrachtet. Der Host verwendet das Integritätszertifikat, um den Schlüsselschutzdienst zur sicheren Freigabe der Schlüssel zu autorisieren, die zur Arbeit mit abgeschirmten virtuellen Computern benötigt werden.

5. Der Host fordert einen VM-Schlüssel an.

Geschützte Hosts besitzen keine Schlüssel zum Einschalten einer abgeschirmten VM (in diesem Fall VM01). Um die erforderlichen Schlüssel zu erhalten, muss der geschützte Host den folgenden KPS bieten:

- Das aktuelle Integritätszertifikat
- Einen verschlüsselten geheimen Schlüssel (Schlüsselschutzvorrichtung oder KP), der die erforderlichen Schlüssel zum Einschalten von VM01 enthält. Der geheime Schlüssel wird mit anderen Schlüsseln verschlüsselt, die nur KPS bekannt sind.

6. Freigabe des Schlüssels.

KPS untersucht das Integritätszertifikat, um seine Gültigkeit zu überprüfen. Das Zertifikat darf nicht abgelaufen sein, und KPS muss dem Nachweisdienst vertrauen, der es ausgestellt hat.

7. Der Schlüssel wird an den Host zurückgegeben.

Wenn das Integritätszertifikat gültig ist, versucht KPS, den geheimen Schlüssel zu entschlüsseln und die zum Einschalten der VM erforderlichen Schlüssel sicher zurückzugeben. Beachten Sie, dass die Schlüssel in den VSB des geschützten Hosts verschlüsselt werden.

8. Host schaltet auf VM01 ein.

Glossar zu geschütztem Fabric und abgeschirmten VMs

BEGRIFF	DEFINITION
Host-Überwachungsdienst (Host Guardian Service, HGS)	Eine Windows Server-Rolle, die auf einem gesicherten Cluster von Bare-Metal-Servern installiert ist, die die Integrität eines Hyper-V-Hosts messen und Schlüssel für fehlerfreie Hyper-V-Hosts freigeben können, wenn sie abgeschirmte VMs einschalten bzw. mit ihnen eine Livemigration durchführen. Diese zwei Funktionen sind ein wesentlicher Bestandteil einer Lösung mit einer abgeschirmten VM und werden als Nachweisdienst und Schlüsselschutzdienst bezeichnet.
geschützter Host	Ein Hyper-V-Host, auf dem abgeschirmte VMs ausgeführt werden können. Ein Host kann nur als <i>geschützt</i> betrachtet werden, wenn er vom HGS-Nachweis Dienst als fehlerfrei eingestuft wurde. Abgeschirmte VMs können nicht eingeschaltet oder live auf einen Hyper-V-Host migriert werden, für den noch kein Nachweis geführt werden konnte, bzw. der den Nachweis nicht erbringen konnte.
geschütztes Fabric	Dies ist der Sammelbegriff zur Beschreibung eines Fabrics mit Hyper-V-Hosts und deren Host-Überwachungsdienst, der die Fähigkeit zum Verwalten und Ausführen abgeschirmter VMs hat.
abgeschirmter virtueller Computer (VM)	Ein virtueller Computer, der nur auf geschützten Hosts ausgeführt werden kann und vor Untersuchung, Manipulation und Diebstahl durch bösartige Fabricadministratoren und Hostmalware geschützt ist.

BEGRIFF	DEFINITION
Fabricadministrator	Ein Public Cloud- oder Private Cloud-Administrator, der virtuelle Computer verwalten kann. Im Rahmen eines geschützten Fabrics hat ein Fabricadministrator keinen Zugriff auf abgeschirmte VMs oder die Richtlinien, die bestimmen, auf welchen Hosts abgeschirmte VMs ausgeführt werden können.
HGS-Administrator	Ein vertrauenswürdiger Administrator in der Public oder Private Cloud, der über die Berechtigung zum Verwalten der Richtlinien und des kryptografischen Materials für geschützte Hosts verfügt, d.h. Hosts, auf denen eine abgeschirmte VM ausgeführt werden kann.
Bereitstellungsdatendatei oder geschützte Datendatei (PDK-Datei)	Eine verschlüsselte Datei, die ein Mandant oder Benutzer erstellt, um wichtige Informationen der VM-Konfiguration zu speichern und vor dem Zugriff anderer Benutzern zu schützen. Eine geschützte Datendatei kann z.B. das Kennwort enthalten, das dem lokalen Administratorkonto zugewiesen wird, wenn die VM erstellt wird.
Virtualisierungsbasierte Sicherheit (VBS)	Eine Hyper-V-basierte Verarbeitungs- und Speicherumgebung, die vor Administratoren geschützt ist. Virtueller sicherer Modus gibt dem System die Möglichkeit zum Speichern von Betriebssystemschlüsseln, die für den Betriebssystemadministrator unsichtbar sind.
virtuelles TPM	Eine virtualisierte Version eines Trusted Platform Module (TPM). Ab Hyper-V in Windows Server 2016 können Sie ein virtuelles TPM 2,0-Gerät bereitstellen, damit virtuelle Computer verschlüsselt werden können, so wie ein physisches TPM die Verschlüsselung eines physischen Computers ermöglicht.

Siehe auch

- [Geschütztes Fabric und abgeschirmte VMs](#)
- Blog: [Daten Center- und Private Cloud-Sicherheitsblog](#)
- Video: [Einführung in abgeschirmte Virtual Machines](#)
- Video: [Einblicke in abgeschirmte VMS mit Windows Server 2016 Hyper-V](#)

Planen eines geschützten Fabrics

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

In den folgenden Themen wird die Planung der Bereitstellung eines geschützten Fabrics und von abgeschirmten virtuellen Computern (VMS) behandelt:

- [Planungs Handbuch für geschütztes Fabric und abgeschirmte VMs für Hoster](#)
- [Kompatible Hardware mit Windows Server 2016 Virtualization-basiertem Schutz der Code Integrität](#)
- [Planungs Handbuch für geschütztes Fabric und abgeschirmte VMs für Mandanten](#)

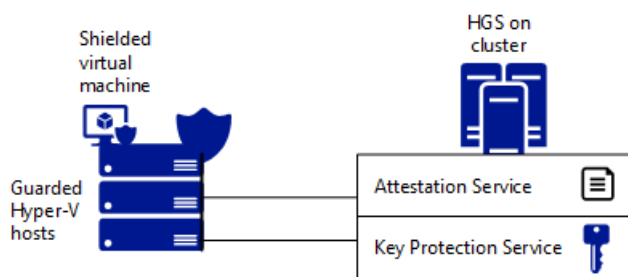
Planungs Handbuch für geschütztes Fabric und abgeschirmte VMs für Hoster

09.04.2020 • 13 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

In diesem Thema werden Planungsentscheidungen behandelt, die vorgenommen werden müssen, damit abgeschirmte virtuelle Maschinen in Ihrem Fabric ausgeführt werden können. Unabhängig davon, ob Sie ein vorhandenes Hyper-V-Fabric aktualisieren oder ein neues Fabric erstellen, besteht das Ausführen von abgeschirmten VMS aus zwei Hauptkomponenten:

- Der Host-Überwachungsdienst (Host Guardian Service, HGS) bietet Nachweis- und Schlüsselschutz, sodass Sie sicherstellen können, dass abgeschirmte VMS nur auf genehmigten und fehlerfreien Hyper-V-Hosts ausgeführt werden.
- Genehmigte und fehlerfreie Hyper-V-Hosts, auf denen abgeschirmte VMS (und reguläre VMS) ausgeführt werden können – diese werden als geschützte Hosts bezeichnet.



Entscheidungs #1: Vertrauens Ebene im Fabric

Die Implementierung des Host-Überwachungs Diensts und der geschützten Hyper-V-Hosts hängt hauptsächlich von der Vertrauens Stärke ab, die Sie in Ihrem Fabric erreichen möchten. Die Stärke der Vertrauensstellung wird durch den Nachweis Modus gesteuert. Es gibt zwei Optionen, die sich gegenseitig ausschließen:

1. TPM-vertrauenswürdiger Nachweis

Wenn Ihr Ziel darin besteht, virtuelle Computer vor böswilligen Administratoren oder einem kompromittierten Fabric zu schützen, verwenden Sie den TPM-vertrauenswürdigen Nachweis. Diese Option eignet sich gut für Szenarien mit mehreren Mandanten und für hochwertige Assets in Unternehmensumgebungen, wie z. B. Domänen Controllern oder Inhalts Servern wie SQL oder SharePoint. Hvci-Richtlinien (Hypervisor-Protected Code Integrity) werden gemessen und deren Gültigkeit durch HGS erzwungen, bevor der Host abgeschirmte VMS ausführen darf.

2. Host Schlüssel Nachweis

Wenn Ihre Anforderungen hauptsächlich von der Konformität abhängig sind, bei der virtuelle Computer sowohl im Ruhezustand als auch in-Flight verschlüsselt werden müssen, verwenden Sie den Host Schlüssel Nachweis. Diese Option eignet sich gut für allgemeine Rechenzentren, in denen Sie mit Hyper-V-Hosts und Fabric-Administratoren vertraut sind, die für tägliche Wartungsarbeiten und Vorgänge auf die Gast Betriebssysteme virtueller Computer zugreifen können.

In diesem Modus ist der Fabric-Administrator allein dafür verantwortlich, die Integrität der Hyper-V-Hosts sicherzustellen. Da HGS bei der Entscheidung, was nicht ausgeführt werden kann, keine Rolle spielt,

funktionieren Schadsoftware und-Debug-Anwendungen wie vorgesehen.

Debugger, die versuchen, direkt an einen Prozess anzufügen (z. b. WinDbg. exe), werden jedoch für abgeschirmte VMS blockiert, da der Arbeitsprozess des virtuellen Computers (VMWP. exe) ein geschütztes Prozess Licht (PPL) ist. Alternative Debuggingtechniken, z. b. die von LiveKd. exe verwendeten, werden nicht blockiert. Anders als bei abgeschirmten VMS wird der Arbeitsprozess für die Verschlüsselung unterstützte VMS nicht als ppl ausgeführt, sodass herkömmliche Debugger wie WinDBG. exe weiterhin normal funktionieren.

Ein ähnlicher Nachweis Modus mit dem Namen admin-Trusted Nachweis (Active Directory basiert) ist ab Windows Server 2019 veraltet.

Die von Ihnen gewählte Vertrauens Ebene übernimmt die Hardwareanforderungen für Ihre Hyper-V-Hosts sowie die Richtlinien, die Sie auf dem Fabric anwenden. Falls erforderlich, können Sie Ihr überwachtes Fabric mit vorhandenem Hardware-und Administrator vertrauenswürdigen Nachweis bereitstellen und dann in einen TPM-vertrauenswürdigen Nachweis konvertieren, wenn die Hardware aktualisiert wurde und Sie die fabricsicherheit verstärken müssen.

Entscheidungs #2: vorhandenes Hyper-v-Fabric im Vergleich zu einem neuen separaten Hyper-v-Fabric

Wenn Sie über ein vorhandenes Fabric (Hyper-V oder anderweitig) verfügen, ist es sehr wahrscheinlich, dass Sie es verwenden können, um abgeschirmte VMS zusammen mit regulären VMS auszuführen. Einige Kunden entscheiden sich dafür, abgeschirmte VMs in Ihre vorhandenen Tools und Fabrics zu integrieren, während andere das Fabric aus geschäftlichen Gründen voneinander trennen.

Planen von HGS-Administratoren für den Host-Überwachungsdienst

Stellen Sie den Host-Überwachungsdienst (Host Guardian Service, HGS) in einer äußerst sicheren Umgebung bereit, egal ob Sie sich auf einem dedizierten physischen Server, einem abgeschirmten virtuellen Computer, einem virtuellen Computer auf einem isolierten Hyper-V-Host (getrennt von dem Fabric, das geschützt ist) oder einem logisch getrennten Azure-Abonnement.

FLÄCHE	DETAILS
Installationsanforderungen	<ul style="list-style-type: none">• Ein Server (Cluster mit drei Knoten wird für Hochverfügbarkeit empfohlen)• Für einen Fallback sind mindestens zwei HGS-Server erforderlich.• Server können entweder virtuell oder physisch (physischer Server mit TPM 2,0 empfohlen) sein. TPM 1,2 wird ebenfalls unterstützt)• Server Core-Installation von Windows Server 2016 oder höher• Netzwerkverbindung mit dem Fabric, das die http-oder Fall Back Konfiguration zulässt• Für die Zugriffs Überprüfung empfohlenes HTTPS-Zertifikat
Größe ändern	Der HGS-Server Knoten der mittleren Größe (8 Kerne/4 GB) kann 1.000 Hyper-V-Hosts verarbeiten.

FLÄCHE	DETAILS
Verwaltung	<p>Bestimmen Sie bestimmte Personen, die HGS verwalten werden. Sie sollten von Fabric-Administratoren getrennt sein. Zum Vergleich können sich HGS-Cluster auf die gleiche Weise wie eine Zertifizierungsstelle (Certificate Authority, ca) im Hinblick auf administrative Isolation, physische Bereitstellung und allgemeine Sicherheits Empfindlichkeit vorstellen.</p>
Active Directory des Host-Überwachungs Diensts	<p>Standardmäßig installiert HGS seine eigenen internen Active Directory für die Verwaltung. Dabei handelt es sich um eine eigenständige, selbstverwaltete Gesamtstruktur, die für die Isolierung von HGS von Ihrem Fabric empfohlen wird.</p> <p>Wenn Sie bereits über eine Active Directory-Gesamtstruktur mit hohen Privilegien verfügen, die Sie für die Isolation verwenden, können Sie diese Gesamtstruktur anstelle der HGS-Standard Gesamtstruktur verwenden. Es ist wichtig, dass HGS nicht zu einer Domäne in derselben Gesamtstruktur wie die Hyper-V-Hosts oder die Fabric-Verwaltungs Tools hinzugefügt werden. Dies könnte einem Fabric-Administrator ermöglichen, die Kontrolle über HGS zu erlangen.</p>
Notfallwiederherstellung	<p>Sie haben drei Möglichkeiten:</p> <ol style="list-style-type: none"> 1. Installieren Sie einen separaten HGS-Cluster in jedem Rechenzentrum, und autorisieren Sie abgeschirmte VMS, die sowohl in den primären als auch in den Sicherungs Datacenter ausgeführt werden. Dadurch ist es nicht mehr erforderlich, den Cluster über ein WAN zu Strecken, und Sie können virtuelle Maschinen so isolieren, dass Sie nur an dem vorgesehenen Standort ausgeführt werden. 2. Installieren Sie HGS in einem Stretch-Cluster zwischen zwei (oder mehr) Rechenzentren. Dies sorgt für Resilienz, wenn das WAN ausfällt, legt jedoch die Grenzen des Failoverclustering fest. Sie können Arbeits Auslastungen nicht zu einem Standort isolieren. eine VM, die zur Laufzeit an einem Standort autorisiert ist, kann auf jedem anderen Standort ausgeführt werden. 3. Registrieren Sie den Hyper-V-Host bei einem anderen HGS als Failover. <p>Sie sollten auch alle HGS sichern, indem Sie die Konfiguration exportieren, sodass Sie jederzeit lokal wieder hergestellt werden können. Weitere Informationen finden Sie unter "Export-hgsserverstate" und "Import-hgsserverstate".</p>

FLÄCHE	DETAILS
Schlüssel des Host-Überwachungs Diensts	<p>Ein Host-Überwachungsdienst verwendet zwei asymmetrische Schlüsselpaare – einen Verschlüsselungsschlüssel und einen Signatur Schlüssel – die jeweils durch ein SSL-Zertifikat dargestellt werden. Es gibt zwei Optionen, um diese Schlüssel zu generieren:</p> <ol style="list-style-type: none"> 1. Interne Zertifizierungsstelle – Sie können diese Schlüssel mithilfe ihrer internen PKI-Infrastruktur generieren. Dies eignet sich für eine Rechenzentrums Umgebung. 2. Öffentlich vertrauenswürdige Zertifizierungsstellen – verwenden Sie einen Satz von Schlüsseln, die von einer öffentlich vertrauenswürdigen Zertifizierungsstelle abgerufen werden. Dies ist die Option, die Hosters verwenden sollten. <p>Beachten Sie, dass es zwar möglich ist, selbst signierte Zertifikate zu verwenden, aber es ist nicht empfehlenswert für andere Bereitstellungs Szenarien als Proof-of-Concept-Labs.</p> <p>Zusätzlich zu den HGS-Schlüsseln kann ein hoester "Bring your own Key" verwenden, wo Mandanten ihre eigenen Schlüssel bereitstellen können, damit einige (oder alle) Mandanten einen eigenen spezifischen HGS-Schlüssel haben können. Diese Option eignet sich für Hosters, die einen Out-of-Band-Prozess für Mandanten bereitstellen können, um Ihre Schlüssel hochzuladen.</p>
Schlüsselspeicher des Host-Überwachungs Diensts	<p>Um die größtmögliche Sicherheit zu erzielen, wird empfohlen, dass HGS-Schlüssel ausschließlich in einem Hardware Sicherheitsmodul (HSM) erstellt und gespeichert werden. Wenn Sie keine HSMs verwenden, wird dringend empfohlen, BitLocker auf den HGS-Servern anzuwenden.</p>

Fabric-Administrator Planung für geschützte Hosts

FLÄCHE	DETAILS
Hardware	<ul style="list-style-type: none"> • Host Schlüssel Nachweis: Sie können eine beliebige vorhandene Hardware als überwachten Host verwenden. Es gibt einige Ausnahmen (um sicherzustellen, dass Ihr Host neue Sicherheitsmechanismen ab Windows Server 2016 verwenden kann, siehe kompatible Hardware mit virtualisierungsbasiertem Windows Server 2016-Schutz der Code Integrität). • TPM-vertrauenswürdiger Nachweis: Sie können jede Hardware verwenden, die über die Hardware Assurance zusätzliche Qualifikation verfügt, sofern diese ordnungsgemäß konfiguriert ist (siehe Server Konfigurationen, die mit abgeschirmten VMS kompatibel sind, und virtualisierungsbasierter Schutz der Code Integrität für die jeweilige Konfiguration). Dies umfasst TPM 2,0 und UEFI, Version 2.3.1 c und höher.
Betriebssystem	<p>Wir empfehlen die Verwendung der Server Core-Option für das Hyper-V-Host Betriebssystem.</p>

FLÄCHE	DETAILS
Auswirkungen auf die Leistung	<p>Auf der Grundlage von Leistungstests erwarten wir einen Dichteunterschied von ungefähr 5% zwischen der Ausführung von abgeschirmten VMS und nicht abgeschirmten VMS. Dies bedeutet Folgendes: Wenn auf einem bestimmten Hyper-V-Host 20 nicht abgeschirmte VMS ausgeführt werden können, wird davon ausgegangen, dass 19 abgeschirmte VMS ausgeführt werden können.</p> <p>Stellen Sie sicher, dass Sie die Größe mit ihren typischen Workloads überprüfen. Beispielsweise gibt es möglicherweise einige Ausreißer mit intensiven Schreib orientierten e/a-Arbeits Auslastungen, die sich weiter auf den Dichteunterschied auswirken.</p>
Überlegungen zu Filialen	<p>Ab Windows Server, Version 1709, können Sie eine Fall Back-URL für einen virtualisierten HGS-Server angeben, der lokal als abgeschirmte VM in der Zweigstelle ausgeführt wird. Die Fall Back-URL kann verwendet werden, wenn die Zweigstelle die Konnektivität mit den HGS-Servern im Daten Center verliert. In früheren Versionen von Windows Server benötigt ein Hyper-V-Host, der in einer Zweigstelle ausgeführt wird, eine Verbindung mit dem Host-Überwachungsdienst, um abgeschirmte VMS einschalten oder Live migrieren zu können. Weitere Informationen finden Sie unter Überlegungen zu Zweigstellen.</p>

Kompatible Hardware mit Windows Server Virtualization-basiertem Schutz der Code Integrität

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

In Windows Server 2016 wurde ein neuer virtualisierungsbasierter Code Schutz eingeführt, um physische und virtuelle Computer vor Angriffen zu schützen, die den Systemcode ändern. Um diese hohe Schutz Ebene zu erreichen, arbeitet Microsoft zusammen mit den Computer Hardwareherstellern (Original Equipment Manufacturers, OEMs) zusammen, um schädliche Schreibvorgänge in den System Ausführungs Code zu verhindern. Dieser Schutz kann auf jedes System angewendet werden und wird als einer der Bausteine für die Implementierung der Hyper-V-Host Integrität für abgeschirmte virtuelle Computer (VMS) verwendet.

Wie bei jedem hardwarebasierten Schutz sind einige Systeme aufgrund von Problemen wie der falschen Markierung von Speicherseiten als ausführbare Dateien oder durch das tatsächliche ändern von Code zur Laufzeit möglicherweise nicht kompatibel. Dies kann zu unerwarteten Fehlern, z. b. Datenverlust oder einem blauen Bildschirm Fehler (auch als "Fehler beim Abbrechen" bezeichnet) führen.

Um kompatibel zu sein und die neue Sicherheitsfunktion vollständig zu unterstützen, müssen OEMs die in UEFI 2,6 definierte Speicher Adress Tabelle implementieren, die in Jan. 2016 veröffentlicht wurde. Die Übernahme des neuen UEFI-Standards nimmt Zeit in Anspruch. um Kunden zu verhindern, dass Probleme auftreten, möchten wir in der Zwischenzeit Informationen über Systeme und Konfigurationen bereitstellen, mit denen wir diese featuremenge getestet haben, sowie über Systeme, die nicht kompatibel sind.

Nicht kompatible Systeme

Die folgenden Konfigurationen sind bekanntermaßen nicht kompatibel mit dem virtualisierungsbasierten Schutz der Code Integrität und können nicht als Host für abgeschirmte VMS verwendet werden:

- Dell PowerEdge-Server, auf denen PERC H330 RAID-Controller ausgeführt werden. Weitere Informationen finden Sie im folgenden Artikel des Dell-Supports [H330 – Aktivieren von "Host-Überwachungs-Hyper-V-Unterstützung" oder "Device Guard" bei Win 2016 OS verursacht Betriebssystem Start Fehler](#).

Kompatible Systeme

Dabei handelt es sich um die Systeme, die wir und unsere Partner in unserer Umgebung getestet haben. Vergewissern Sie sich, dass das System in Ihrer Umgebung erwartungsgemäß funktioniert:

- Virtual Machines – Sie können den virtualisierungsbasierten Schutz der Code Integrität auf virtuellen Computern aktivieren, die auf einem Hyper-V-Host ab Windows Server 2016 ausgeführt werden.

Planungs Handbuch für geschütztes Fabric und abgeschirmte VMs für Mandanten

09.04.2020 • 12 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Dieses Thema konzentriert sich auf VM-Besitzer, die Ihre virtuellen Computer (Virtual Machines, VMS) zu Kompatibilitäts- und Sicherheitszwecken schützen möchten. Unabhängig davon, ob die virtuellen Computer auf dem geschützten Fabric eines Hostinganbieters oder einem privaten geschützten Fabric ausgeführt werden, müssen die VM-Besitzer die Sicherheitsstufe ihrer abgeschirmten VMS steuern. Dazu gehört auch die Beibehaltung der Möglichkeit, Sie bei Bedarf zu entschlüsseln.

Bei der Verwendung von abgeschirmten VMS sind drei Bereiche zu beachten:

- Die Sicherheitsstufe für die VMs
- Die kryptografischen Schlüssel, mit denen Sie geschützt werden.
- Schutz Daten – vertrauliche Informationen, die zum Erstellen von abgeschirmten VMS verwendet werden

Sicherheitsstufe für die VMs

Beim Bereitstellen von abgeschirmten VMS muss eine von zwei Sicherheitsstufen ausgewählt werden:

- Abgesch
- Verschlüsselung unterstützt

Sowohl abgeschirmte als auch durch Verschlüsselung unterstützte VMS sind einem virtuellen TPM angefügt, und diejenigen, die Windows ausführen, werden durch BitLocker geschützt. Der Hauptunterschied besteht darin, dass abgeschirmte VMS den Zugriff durch Fabric-Administratoren blockieren, während von Verschlüsselung gestützten VMS Fabric-Administratoren die gleiche Zugriffsebene wie bei einer regulären VM gestattet wird. Weitere Informationen zu diesen Unterschieden finden Sie unter [Übersicht über geschützte Fabric und abgeschirmte VMS](#).

Wählen Sie **abgeschirmte VMS** aus, wenn Sie den virtuellen Computer vor einem kompromittierten Fabric schützen möchten (einschließlich kompromittierter Administratoren). Sie sollten in Umgebungen verwendet werden, in denen Fabric-Administratoren und das Fabric selbst nicht vertrauenswürdig sind. Wählen Sie **Verschlüsselung unterstützte VMS** aus, wenn Sie eine Kompatibilitäts Leiste erreichen möchten, die ggf. Verschlüsselung ruhender Daten und Verschlüsselung des virtuellen Computers (z. B. während der Live Migration) erfordert.

Durch Verschlüsselung unterstützte VMS sind ideal in Umgebungen, in denen Fabric-Administratoren voll vertrauenswürdig sind, die Verschlüsselung jedoch weiterhin erforderlich ist.

Sie können eine Mischung aus regulären VMS, abgeschirmten VMS und von der Verschlüsselung unterstützten VMs in einem geschützten Fabric und sogar auf demselben Hyper-V-Host ausführen.

Ob ein virtueller Computer abgeschirmt oder die Verschlüsselung unterstützt wird, hängt von den geschützten Daten ab, die beim Erstellen des virtuellen Computers ausgewählt werden. VM-Besitzer konfigurieren die Sicherheitsstufe beim Erstellen der geschützten Daten (siehe Abschnitt "Schutz [Daten](#)"). Beachten Sie, dass diese Option nicht geändert werden kann, wenn die VM im Virtualisierungsfabric verbleibt.

Für abgeschirmte VMS verwendete kryptografische Schlüssel

Abgeschirmte VMS sind vor virtualisierungsfabric-Angriffsvektoren mithilfe verschlüsselter Datenträger und verschiedener anderer verschlüsselter Elemente geschützt, die nur entschlüsselt werden können:

- **Einen Besitzer Schlüssel** – Dies ist ein kryptografischer Schlüssel, der vom VM-Besitzer verwaltet wird und in der Regel für die letzte Wiederherstellung oder Problembehandlung verwendet wird. VM-Besitzer sind verantwortlich für die Verwaltung von Besitzer Schlüsseln an einem sicheren Ort.
- **Mindestens ein Wächter (Host-Überwachungs Schlüssel)** – jeder Wächter stellt ein virtualisierungsfabric dar, in dem ein Besitzer abgeschirmte VMs für die Durchführung autorisiert. Unternehmen verfügen häufig über ein primäres und Notfall Wiederherstellungs Fabric (Disaster Recovery, Dr) und autorisieren Ihre abgeschirmten VMs in der Regel auf beiden Computern. In einigen Fällen kann das sekundäre Fabric (Dr) von einem Public Cloud-Anbieter gehostet werden. Die privaten Schlüssel für ein beliebiges geschütztes Fabric werden nur im virtualisierungsfabric verwaltet, während ihre öffentlichen Schlüssel heruntergeladen werden können und in Ihrem Wächter enthalten sind.

Gewusst wie einen Besitzer Schlüssel erstellen? Ein Besitzer Schlüssel wird durch zwei Zertifikate repräsentiert. Ein Zertifikat für die Verschlüsselung und ein Zertifikat für die Signierung. Sie können diese beiden Zertifikate mithilfe ihrer eigenen PKI-Infrastruktur erstellen oder SSL-Zertifikate von einer öffentlichen Zertifizierungsstelle (ca) abrufen. Zu Testzwecken können Sie auch ein selbst signiertes Zertifikat auf allen Computern erstellen, die mit Windows 10 oder Windows Server 2016 beginnen.

Wie viele Besitzer Schlüssel sollten Sie haben? Sie können einen einzelnen Besitzer Schlüssel oder mehrere Besitzer Schlüssel verwenden. Bewährte Methoden empfehlen einen einzelnen Besitzer Schlüssel für eine Gruppe von virtuellen Computern, die die gleiche Sicherheit, Vertrauensstufe und Risikostufe und für administrative Kontrolle haben. Sie können einen einzelnen Besitzer Schlüssel für alle in die Domäne eingebundenen abgeschirmten VMS freigeben und diesen Besitzer Schlüssel zur Verwaltung durch die Domänen Administratoren hinterlegen.

Kann ich meine eigenen Schlüssel für den Host-Wächter verwenden? Ja, Sie können Ihren eigenen Schlüssel in den Hostinganbieter einbringen und diesen Schlüssel für Ihre abgeschirmten VMS verwenden. Dies ermöglicht Ihnen die Verwendung ihrer speziellen Schlüssel (im Gegensatz zum Verwenden des Hostinganbieters) und kann verwendet werden, wenn Sie über bestimmte Sicherheits- oder Sicherheitsbestimmungen verfügen, die Sie einhalten müssen. Aus Gründen der Schlüssel Pflege sollten sich die Host-Überwachungs Schlüssel vom Besitzer Schlüssel unterscheiden.

Geschützte Daten

Geschützte Daten enthalten die geheimen Schlüssel, die für die Bereitstellung von abgeschirmten oder Verschlüsselungs gestützten VMS erforderlich sind. Sie wird auch verwendet, wenn reguläre VMs in abgeschirmte VMS umgerechnet werden.

Geschützte Daten werden mithilfe des Assistenten zum Schützen von Datendateien erstellt und in PDK-Dateien gespeichert, die von VM-Besitzern in das geschützte Fabric hochgeladen werden.

Abgeschirmte VMS tragen zum Schutz vor Angriffen von einem kompromittierten virtualisierungsfabric bei. Daher benötigen wir einen sicheren Mechanismus, um sensible Initialisierungs Daten zu übergeben, z. b. das Administrator Kennwort, Anmelde Informationen für den Domänen Beitritt oder RDP-Zertifikate, ohne dass diese dem virtualisierungsfabric selbst oder den Administratoren offen liegen. Außerdem enthalten die geschützten Daten Folgendes:

1. Sicherheitsstufe – abgeschirmt oder Verschlüsselung unterstützt
2. Besitzer und Liste der vertrauenswürdigen hostwächter, auf denen die VM ausgeführt werden kann
3. Initialisierungs Daten für virtuelle Computer ("Unattend.xml", RDP-Zertifikat)
4. Liste der vertrauenswürdigen signierten Vorlagen Datenträger zum Erstellen der VM in der Virtualisierungsumgebung

Wenn Sie einen geschützten oder Verschlüsselungs gestützten virtuellen Computer erstellen oder einen vorhandenen virtuellen Computer umrechnen, werden Sie aufgefordert, die geschützten Daten auszuwählen, anstatt zur Angabe der sensiblen Informationen aufgefordert zu werden.

Wie viele geschützte Datendateien benötige ich? Sie können eine einzelne geschützte Datendatei zum Erstellen jeder abgeschirmten VM verwenden. Wenn eine bestimmte abgeschirmte VM jedoch erfordert, dass eines der vier Elemente anders ist, ist eine zusätzliche Schutz Datendatei erforderlich. Angenommen, Sie verfügen über eine Schutz Datendatei für Ihre IT-Abteilung und eine andere Schutz Datendatei für die Personalabteilung, da Ihr anfängliches Administrator Kennwort und RDP-Zertifikate voneinander abweichen.

Die Verwendung separater Schutz Datendateien für jede abgeschirmte VM ist zwar möglich, ist aber nicht unbedingt die optimale Wahl und sollte aus den richtigen Gründen erfolgen. Wenn z. b. jeder geschützte virtuelle Computer über ein anderes Administrator Kennwort verfügen muss, sollten Sie stattdessen einen Kenn Wort Verwaltungsdienst oder ein Tool wie [die lokale Administrator Kennwort-Lösung \(Runden\) von Microsoft](#) verwenden.

Erstellen einer abgeschirmten VM in einem virtualisierungsfabric

Es gibt mehrere Optionen zum Erstellen einer abgeschirmten VM in einem virtualisierungsfabric (Folgendes ist für abgeschirmte und durch Verschlüsselung unterstützte VMS relevant):

1. Erstellen einer abgeschirmten VM in Ihrer Umgebung und Hochladen der VM in das virtualisierungsfabric
2. Erstellen einer neuen abgeschirmten VM aus einer signierten Vorlage auf dem virtualisierungsfabric
3. Schützen eines vorhandenen virtuellen Computers (die vorhandene VM muss die Generation 2 sein und Windows Server 2012 oder höher ausführen)

Das Erstellen neuer virtueller Computer aus einer Vorlage ist üblich. Da sich der Vorlagen Datenträger, der zum Erstellen einer neuen abgeschirmten VM verwendet wird, auf dem virtualisierungsfabric befindet, sind jedoch zusätzliche Maßnahmen erforderlich, um sicherzustellen, dass er nicht von einem böswilligen Fabric-Administrator oder von Schadsoftware manipuliert wurde, die auf dem Fabric ausgeführt wird. Dieses Problem wird mithilfe von signierten Vorlagen Datenträgern gelöst – signierte Vorlagen Datenträger und deren Datenträger Signaturen werden von vertrauenswürdigen Administratoren oder dem Besitzer der VM erstellt. Wenn eine abgeschirmte VM erstellt wird, wird die Signatur des Vorlagen Datenträgers mit den Signaturen in der angegebenen Schutz Datendatei verglichen. Wenn eine der Signaturen der Schutz Datendatei mit der Signatur des Vorlagen Datenträgers identisch ist, wird der Bereitstellungs Prozess fortgesetzt. Wenn keine Entsprechung gefunden werden kann, wird der Bereitstellungs Prozess abgebrochen, um sicherzustellen, dass die VM-Geheimnisse aufgrund eines nicht vertrauenswürdigen Vorlagen Datenträgers nicht beeinträchtigt werden.

Wenn Sie signierte Vorlagen Datenträger verwenden, um geschützte VMS zu erstellen, sind zwei Optionen verfügbar:

1. Verwenden Sie einen vorhandenen signierten Vorlagen Datenträger, der vom Virtualisierungsanbieter bereitgestellt wird. In diesem Fall verwaltet der Virtualisierungsanbieter signierte Vorlagen Datenträger.
2. Hochladen eines signierten Vorlagen Datenträgers in das virtualisierungsfabric. Der Besitzer der VM ist für die Verwaltung signierter Vorlagen Datenträger verantwortlich.

Bereitstellen des Host-Überwachungs Diensts

09.04.2020 • 2 minutes to read • [Edit Online](#)









Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016














Eines der wichtigsten Ziele bei der Bereitstellung einer gehosteten Umgebung besteht darin, die Sicherheit der virtuellen Computer zu gewährleisten, die in der Umgebung ausgeführt werden. Als Cloud-Dienstanbieter oder privater Cloud-Administrator im Unternehmen können Sie ein geschütztes Fabric verwenden, um eine sicherere Umgebung für VMs bereitzustellen. Ein geschütztes Fabric besteht aus einem Host Guardian Service (Host-Überwachungsdienst) – in der Regel ein Cluster mit drei Knoten – sowie einem oder mehreren geschützten Hosts und einer Reihe von abgeschirmten virtuellen Computern (VMs).

Video: Bereitstellen eines geschützten Fabric

Bereitstellungs Aufgaben für geschützte Fabric und abgeschirmte VMS

In der folgenden Tabelle werden die Aufgaben zum Bereitstellen eines geschützten Fabric und zum Erstellen von abgeschirmten VMS entsprechend den verschiedenen Administrator Rollen aufgegliedert. Beachten Sie Folgendes: Wenn der HGS-Administrator HGS mit autorisierten Hyper-V-Hosts konfiguriert, sammelt ein Fabric-Administrator Informationen zu den Hosts gleichzeitig und stellt diese bereit.

 Host guardian service administrator tasks	 Fabric administrator tasks	 Tenant administrator tasks
(1) Überprüfen der HGS-Voraussetzungen 		
(2) Konfigurieren des ersten HGS Knoten 		
(3) Konfigurieren zusätzlicher HGS Knoten 		
	(4) Konfigurieren des Fabric-DNS 	
	(5) Überprüfen der Voraussetzungen für Host (Schlüssel) Überprüfen der Host Voraussetzungen (TPM) 	

 Host guardian service administrator tasks	 Fabric administrator tasks	 Tenant administrator tasks
(7) Konfigurieren von HGS mit Hostinformationen 	(6) Erstellen eines Host Schlüssels (Schlüssel) Sammeln von Hostinformationen (TPM) 	
	(8) bestätigen, dass Hosts bestätigen können 	
	(9) Konfigurieren von VMM (optional) 	
	(10) Erstellen von Vorlagen Datenträgern 	
	(11) Erstellen eines VM-schutzhilfsobjekts für VMM (optional) 	
	(12) Einrichten Windows Azure Pack (optional) 	
		(13) Schutz Datendatei erstellen 
		(14) Erstellen von abgeschirmten VMS mithilfe Windows Azure Pack Erstellen von abgeschirmten VMS mithilfe von VMM  

Siehe auch

- [Geschütztes Fabric und abgeschirmte VMs](#)

Schnellstart für die geschützte Fabric-Bereitstellung

09.04.2020 • 15 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema wird erläutert, was ein geschütztes Fabric ist, seine Anforderungen und eine Zusammenfassung des Bereitstellungs Prozesses. Ausführliche Informationen zur Bereitstellung finden Sie unter Bereitstellen [des Host-Überwachungs Diensts für überwachte Hosts und abgeschirmte VMS](#).

Lieber ein Video ansehen? Weitere Informationen finden Sie im Microsoft Virtual Academy-Kurs bereitstellen [von abgeschirmten VMS und einem geschützten Fabric mit Windows Server 2016](#).

Was ist ein geschütztes Fabric?

Bei einem *geschützten Fabric* handelt es sich um ein Windows Server 2016 Hyper-V-Fabric, mit dem mandantenworkloads vor Untersuchung, Diebstahl und Manipulation durch Schadsoftware, die auf dem Host ausgeführt wird, sowie von Systemadministratoren geschützt werden können. Diese virtualisierten mandantenworkloads – sowohl im Ruhezustand als auch in-Flight – werden als *_abgeschirmte VMS_* bezeichnet.

Welche Anforderungen gelten für ein geschütztes Fabric?

Zu den Anforderungen für ein überwacht Fabric gehören:

- **Ein Ort zum Ausführen von abgeschirmten VMS, die kostenlos von Schadsoftware ausgeführt werden.**

Diese werden als *_geschützte Hosts_* bezeichnet. Geschützte Hosts sind Windows Server 2016 Datacenter Edition Hyper-V-Hosts, die abgeschirmte VMS nur ausführen können, wenn Sie beweisen können, dass Sie in einem bekannten und vertrauenswürdigen Zustand einer externen Zertifizierungsstelle ausgeführt werden, die als Host-Überwachungsdienst (Host-Überwachungsdienst) bezeichnet wird. Die HGS ist eine neue Server Rolle in Windows Server 2016 und wird in der Regel als Cluster mit drei Knoten bereitgestellt.

- **Eine Möglichkeit zum Überprüfen, ob sich ein Host in einem fehlerfreien Zustand befindet.**

Die HGS führt *_einen_Nachweis_* durch, wobei die Integrität der überwachten Hosts gemessen wird.

- **Ein Prozess, mit dem Schlüssel für fehlerfreie Hosts sicher freigegeben werden.**

Die HGS führen den *_Schlüsselschutz_* und die *schlüssel freigabe_aus_*, bei denen die Schlüssel wieder für fehlerfreie Hosts freigegeben werden.

- **Verwaltungs Tools zum Automatisieren der sicheren Bereitstellung und des Hostings von abgeschirmten VMS.**

Optional können Sie diese Verwaltungs Tools einem geschützten Fabric hinzufügen:

- System Center 2016 Virtual Machine Manager (VMM). VMM wird empfohlen, da Sie zusätzliche Verwaltungs Tools bereitstellt, die über das, was Sie bei der Verwendung von PowerShell-Cmdlets, die mit Hyper-V und den geschützten Fabric-Workloads geliefert werden, hinausgehen.
- System Center 2016 Service Provider Foundation (SPF). Dies ist eine API-Schicht zwischen Windows Azure Pack und VMM und eine Voraussetzung für die Verwendung von Windows Azure Pack.
- Windows Azure Pack bietet eine gute grafische Webschnittstelle zum Verwalten eines geschützten Fabrics und geschützter VMS.

In der Praxis muss eine Entscheidung im Vordergrund getroffen werden: der Nachweis [Modus](#), der vom geschützten Fabric verwendet wird. Es gibt zwei Möglichkeiten – zwei sich gegenseitig ausschließende Modi –, mit denen HGS messen kann, dass ein Hyper-V-Host fehlerfrei ist. Wenn Sie HGS initialisieren, müssen Sie den folgenden Modus auswählen:

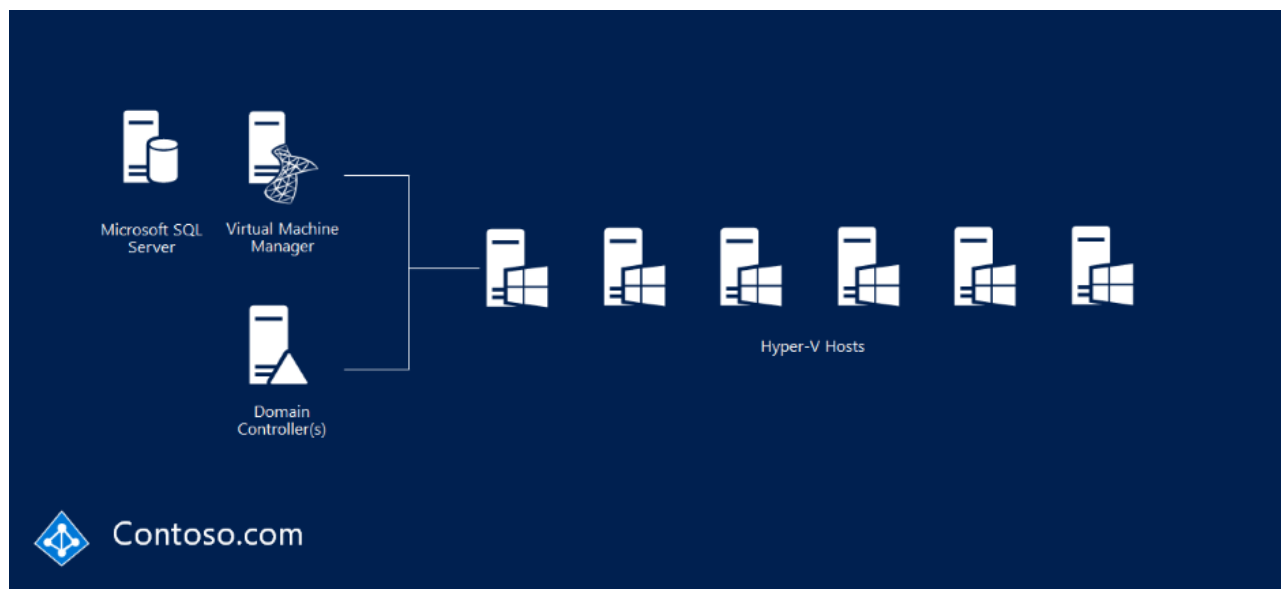
- Der Host Schlüssel Nachweis oder Schlüssel Modus ist weniger sicher, aber leichter zu übernehmen.
- Der TPM-basierte Nachweis oder der TPM-Modus ist sicherer, erfordert jedoch mehr Konfiguration und spezielle Hardware

Falls erforderlich, können Sie die Bereitstellung im Schlüssel Modus mithilfe vorhandener Hyper-V-Hosts durchführen, die auf Windows Server 2019 Datacenter Edition aktualisiert wurden, und dann in den sichereren TPM-Modus konvertieren, wenn die Server Hardware (einschließlich TPM 2,0) unterstützt wird.

Nun, da Sie wissen, was die Teile sind, sehen wir uns ein Beispiel für das Bereitstellungs Modell an.

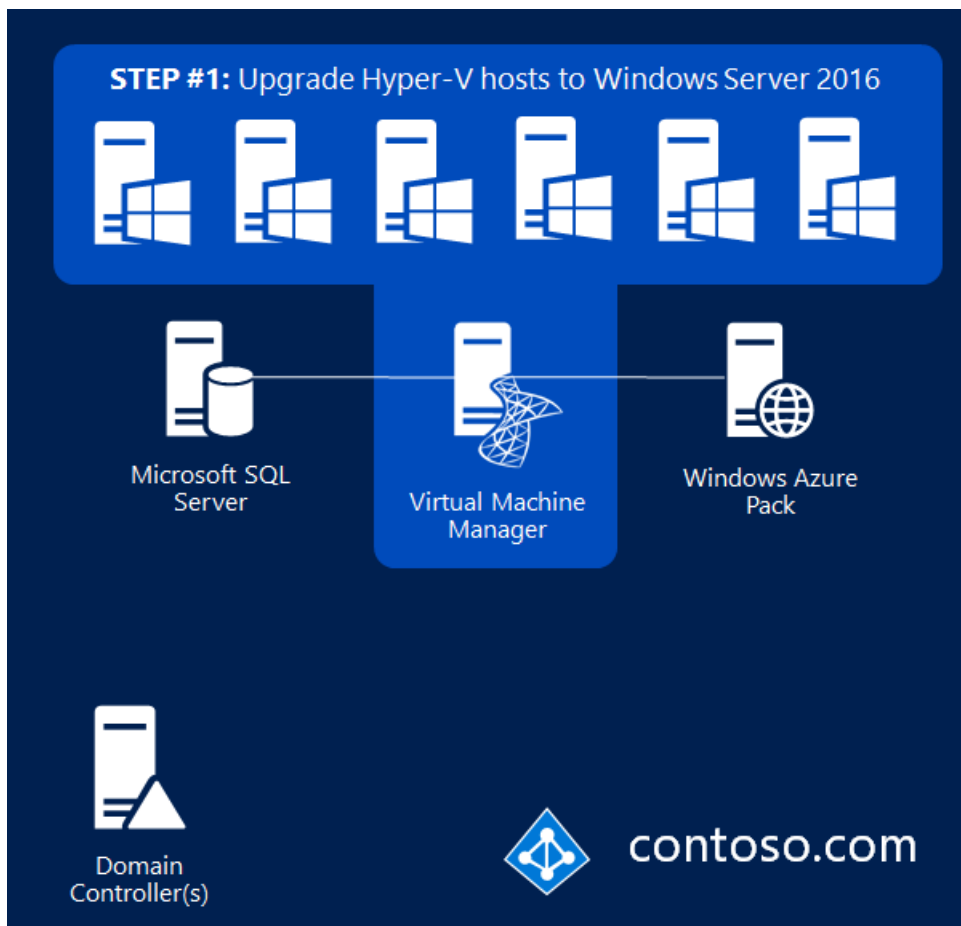
So gelangen Sie von einem aktuellen Hyper-V-Fabric zu einem geschützten Fabric

Stellen Sie sich dieses Szenario vor – Sie haben ein vorhandenes Hyper-V-Fabric, wie z. b. contoso.com in der folgenden Abbildung, und Sie möchten ein geschütztes Windows Server 2016-Fabric erstellen.



Schritt 1: Bereitstellen der Hyper-V-Hosts unter Windows Server 2016

Auf den Hyper-V-Hosts muss Windows Server 2016 Datacenter Edition oder höher ausgeführt werden. Wenn Sie Hosts aktualisieren, können Sie ein [Upgrade](#) von der Standard Edition auf Datacenter Edition durchführen.



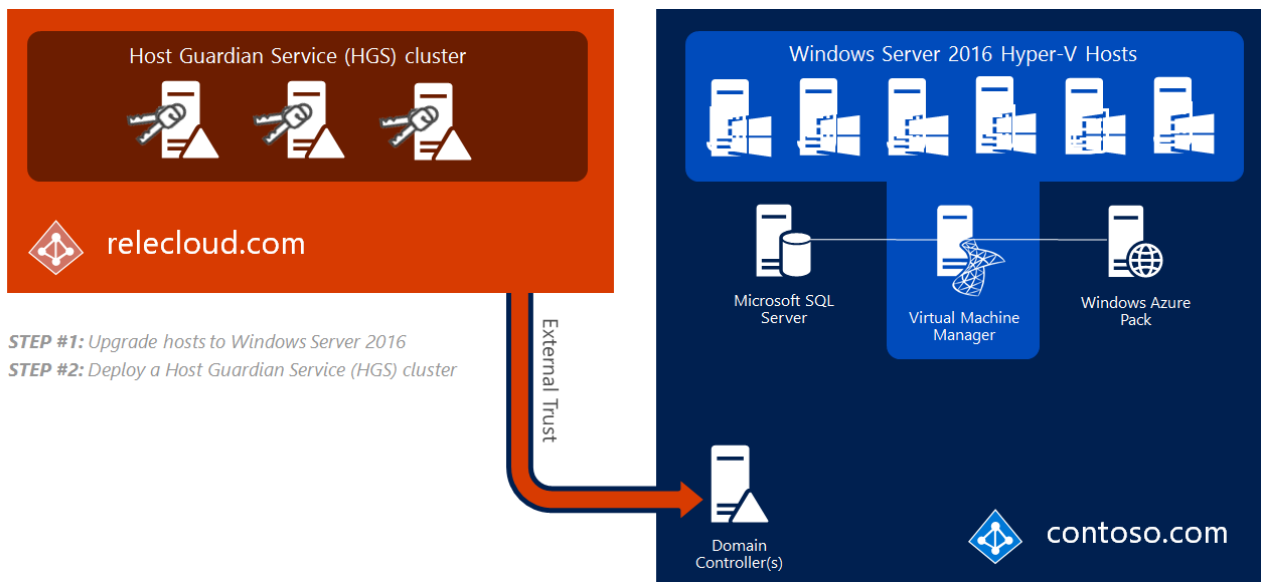
Schritt 2: Bereitstellen des Host-Überwachungs Diensts (HGS)

Installieren Sie dann die HGS-Server Rolle, und stellen Sie Sie als Cluster mit drei Knoten bereit, wie z. b. das relecloud.com-Beispiel in der folgenden Abbildung. Hierfür sind drei PowerShell-Cmdlets erforderlich:

- Verwenden Sie zum Hinzufügen der HGS-Rolle `Install-WindowsFeature`
- Verwenden Sie zum Installieren der HGS `Install-HgsServer`
- Um die HGS mit dem gewählten Nachweis Modus zu initialisieren, verwenden Sie `Initialize-HgsServer`

Wenn Ihre vorhandenen Hyper-V-Server die Voraussetzungen für den TPM-Modus nicht erfüllen (z. b. Wenn Sie nicht über TPM 2,0 verfügen), können Sie HGS mit dem Administrator basierten Nachweis (AD-Modus) initialisieren, für den eine Active Directory Vertrauensstellung mit der Fabric-Domäne erforderlich ist.

Nehmen wir in unserem Beispiel an, dass "Configuration Manager" zuerst im AD-Modus bereitgestellt wird, um die Konformitätsanforderungen sofort zu erfüllen, und plant die Konvertierung in den sichereren TPM-basierten Nachweis, nachdem die geeignete Server Hardware erworben werden kann.



Schritt 3: Extrahieren von Identitäten, hardwarebaselines und Code Integritäts Richtlinien

Der Prozess zum Extrahieren von Identitäten von Hyper-V-Hosts hängt vom verwendeten Nachweis Modus ab.

Für den AD-Modus ist die ID des Hosts das in die Domäne eingebundenen Computer Konto, das Mitglied einer bestimmten Sicherheitsgruppe in der Fabric-Domäne sein muss. Die Mitgliedschaft in der angegebenen Gruppe ist die einzige Bestimmung, ob der Host fehlerfrei ist oder nicht.

In diesem Modus ist der Fabric-Administrator allein dafür verantwortlich, die Integrität der Hyper-V-Hosts sicherzustellen. Da HGS bei der Entscheidung, was nicht ausgeführt werden kann, keine Rolle spielt, funktionieren Schadsoftware und-Debug-Anwendungen wie vorgesehen.

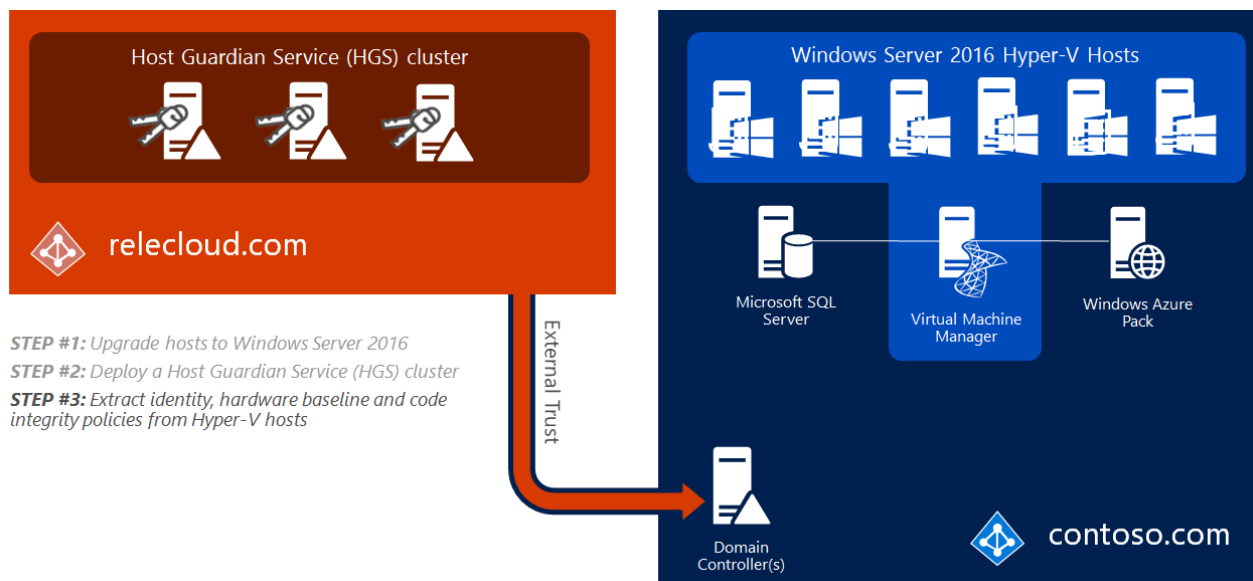
Debugger, die versuchen, direkt an einen Prozess anzufügen (z. b. WinDbg. exe), werden jedoch für abgeschirmte VMS blockiert, da der Arbeitsprozess des virtuellen Computers (VMWP. exe) ein geschütztes Prozess Licht (PPL) ist. Alternative Debuggingtechniken, z. b. die von LiveKd. exe verwendeten, werden nicht blockiert. Anders als bei abgeschirmten VMS wird der Arbeitsprozess für die Verschlüsselung unterstützte VMS nicht als ppl ausgeführt, sodass herkömmliche Debugger wie WinDBG. exe weiterhin normal funktionieren.

Anders ausgedrückt: die strengen Validierungs Schritte, die für den TPM-Modus verwendet werden, werden in keiner Weise für den AD-Modus verwendet.

Für den TPM-Modus sind drei Schritte erforderlich:

1. Einen *öffentlichen Endorsement Key* (oder *ekpub*) von TPM 2,0 auf jedem und jedem Hyper-V-Host. Verwenden Sie zum Erfassen der `ekpub-Get-PlatformIdentifier`.
2. Eine *hardwarebaseline*. Wenn jeder ihrer Hyper-V-Hosts identisch ist, benötigen Sie nur eine einzige Baseline. Wenn dies nicht der Fall ist, benötigen Sie für jede Hardware Klasse einen. Die Baseline hat die Form einer Trusted Computing Group Logfile oder `tcglog`. `Tcglog` enthält alle Elemente, die der Host von der UEFI-Firmware über den Kernel verwendet hat, und zwar direkt bis zu dem Ort, an dem der Host vollständig gestartet wurde. Zum Erfassen der hardwarebaseline installieren Sie die Hyper-v-Rolle und die Hyper-v-Unterstützung des Host-Überwachungs Diensts und verwenden `Get-HgsAttestationBaselinePolicy`.
3. Eine *Code Integritätsrichtlinie*. Wenn jeder ihrer Hyper-V-Hosts identisch ist, benötigen Sie nur eine einzige CI-Richtlinie. Wenn dies nicht der Fall ist, benötigen Sie für jede Hardware Klasse einen. Windows Server 2016 und Windows 10 verfügen jeweils über eine neue Form der Erzwingung für CI-Richtlinien, die als *Hypervisor-erzwungene Code Integrität* (*hvci*) bezeichnet wird. *Hvci* bietet eine starke Erzwingung und stellt sicher, dass ein Host nur Binärdateien ausführen darf, die von einem vertrauenswürdigen Administrator ausgeführt werden dürfen. Diese Anweisungen sind in einer CI-Richtlinie umschließt, die zu HGS hinzugefügt wird. HGS misst die

CI-Richtlinie jedes Hosts, bevor Sie geschützte VMS ausführen dürfen. Verwenden Sie zum Erfassen einer CI-Richtlinie `New-CIPolicy`. Die Richtlinie muss dann mithilfe von `ConvertFrom-CIPolicy` in das binäre Formular konvertiert werden.



Das ist alles – das geschützte Fabric wird in Bezug auf die Infrastruktur für die Durchführung erstellt. Nun können Sie einen abgeschirmten VM-Vorlagen Datenträger und eine geschützte Datendatei erstellen, damit abgeschirmte VMS einfach und sicher bereitgestellt werden können.

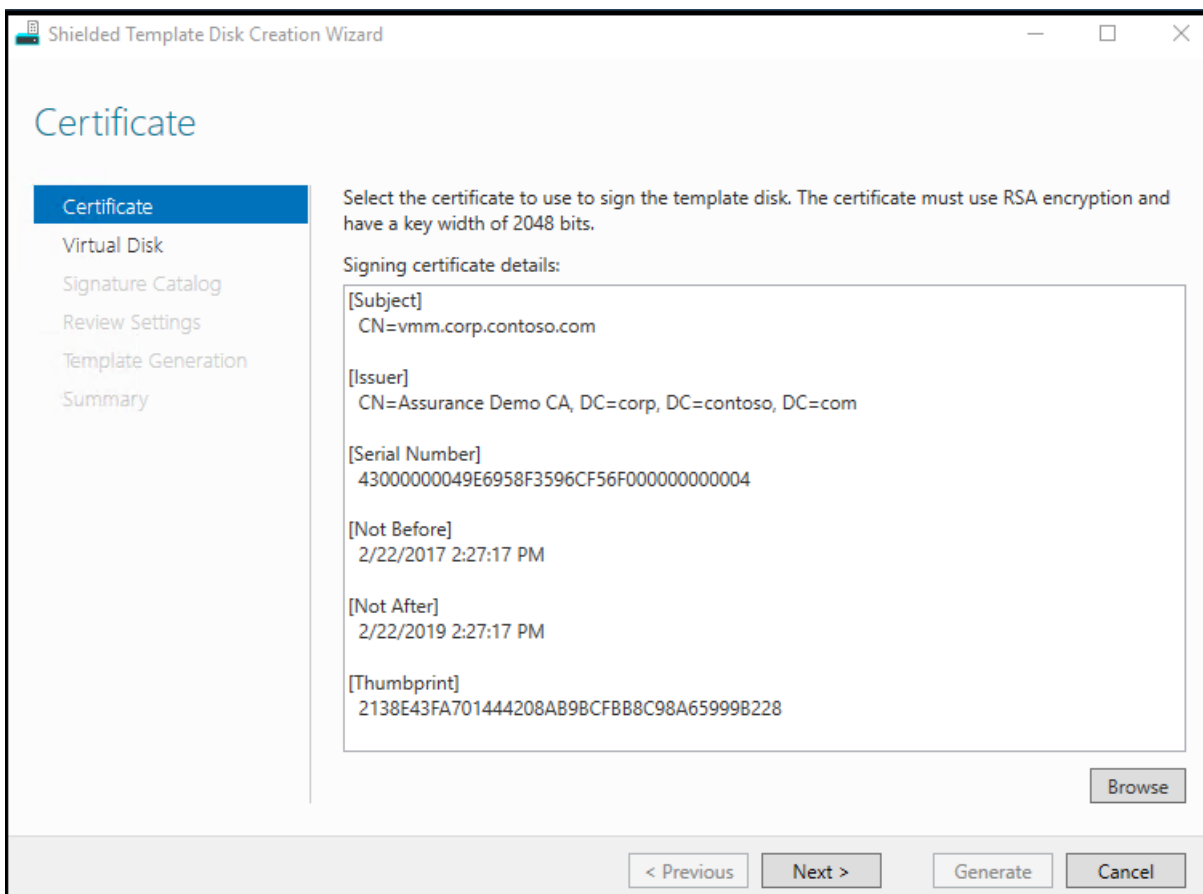
Schritt 4: Erstellen einer Vorlage für abgeschirmte VMS

Eine geschützte VM-Vorlage schützt Vorlagen Datenträger, indem eine Signatur des Datenträgers zu einem bekannten vertrauenswürdigen Zeitpunkt erstellt wird. Wenn der Vorlagen Datenträger später durch Schadsoftware infiziert wird, unterscheidet sich seine Signatur von der ursprünglichen Vorlage, die durch den sicheren abgeschirmten VM-Bereitstellungs Prozess erkannt wird. Geschützte Vorlagen Datenträger werden erstellt, indem der **Assistent zum Erstellen einer abgeschirmten Vorlage** oder eine `Protect-TemplateDisk` auf einem regulären Vorlagen Datenträger

Jede ist in der [Remoteserver-Verwaltungstools für Windows 10](#) in der Funktion der **abgeschirmten VM-Tools** enthalten. Nachdem Sie RSAT heruntergeladen haben, führen Sie den folgenden Befehl aus, um das Feature der **abgeschirmten VM-Tools**

```
Install-WindowsFeature RSAT-Shielded-VM-Tools -Restart
```

Ein vertrauenswürdiger Administrator (z. b. der Fabric-Administrator oder der Besitzer der VM) benötigt ein Zertifikat (häufig von einem hostingdienstanbieter bereitgestellt) zum Signieren des vhdx-Vorlagen Datenträgers

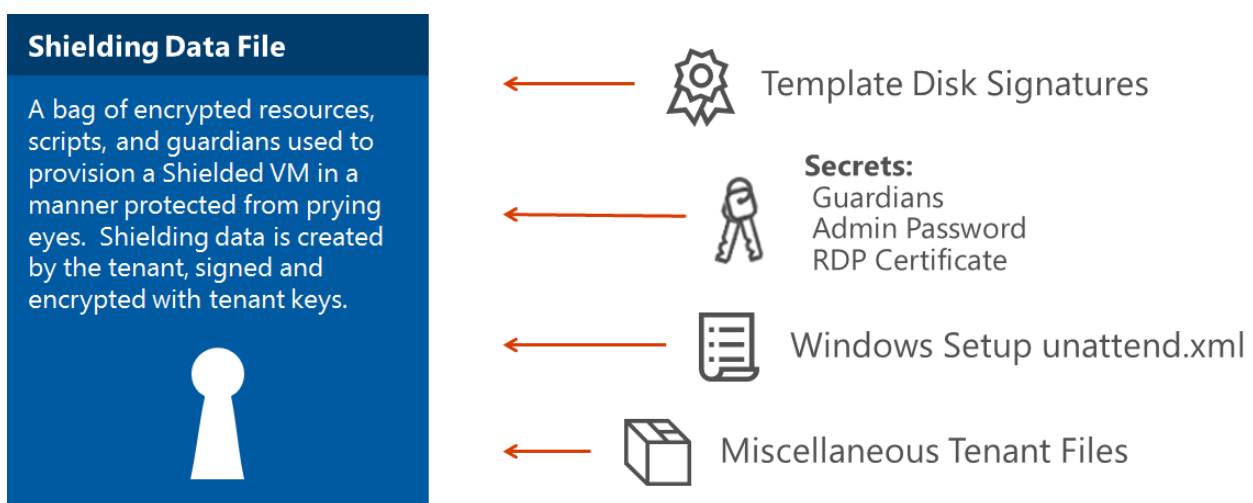


Die Datenträger Signatur wird über die Betriebssystem Partition des virtuellen Datenträgers berechnet. Wenn Änderungen an der Betriebssystem Partition vorgenommen werden, ändert sich auch die Signatur. Dies ermöglicht es Benutzern, die entsprechenden Datenträger durch Angabe der entsprechenden Signatur stark zu identifizieren.

Überprüfen Sie die [Vorlagen Anforderungen](#) für Datenträger, bevor Sie loslegen.

Schritt 5: Erstellen einer Schutz Datendatei

Eine geschützte Datendatei, die auch als PDK-Datei bezeichnet wird, erfasst vertrauliche Informationen über den virtuellen Computer, z. b. das Administrator Kennwort.



Die Schutz Datendatei enthält auch die Sicherheitsrichtlinien Einstellung für den abgeschirmten virtuellen Computer. Wenn Sie eine geschützte Datendatei erstellen, müssen Sie eine von zwei Sicherheitsrichtlinien auswählen:

- Abgesch

Die sicherste Option, bei der viele administrative Angriffsvektoren vermieden werden.

- Verschlüsselung unterstützt

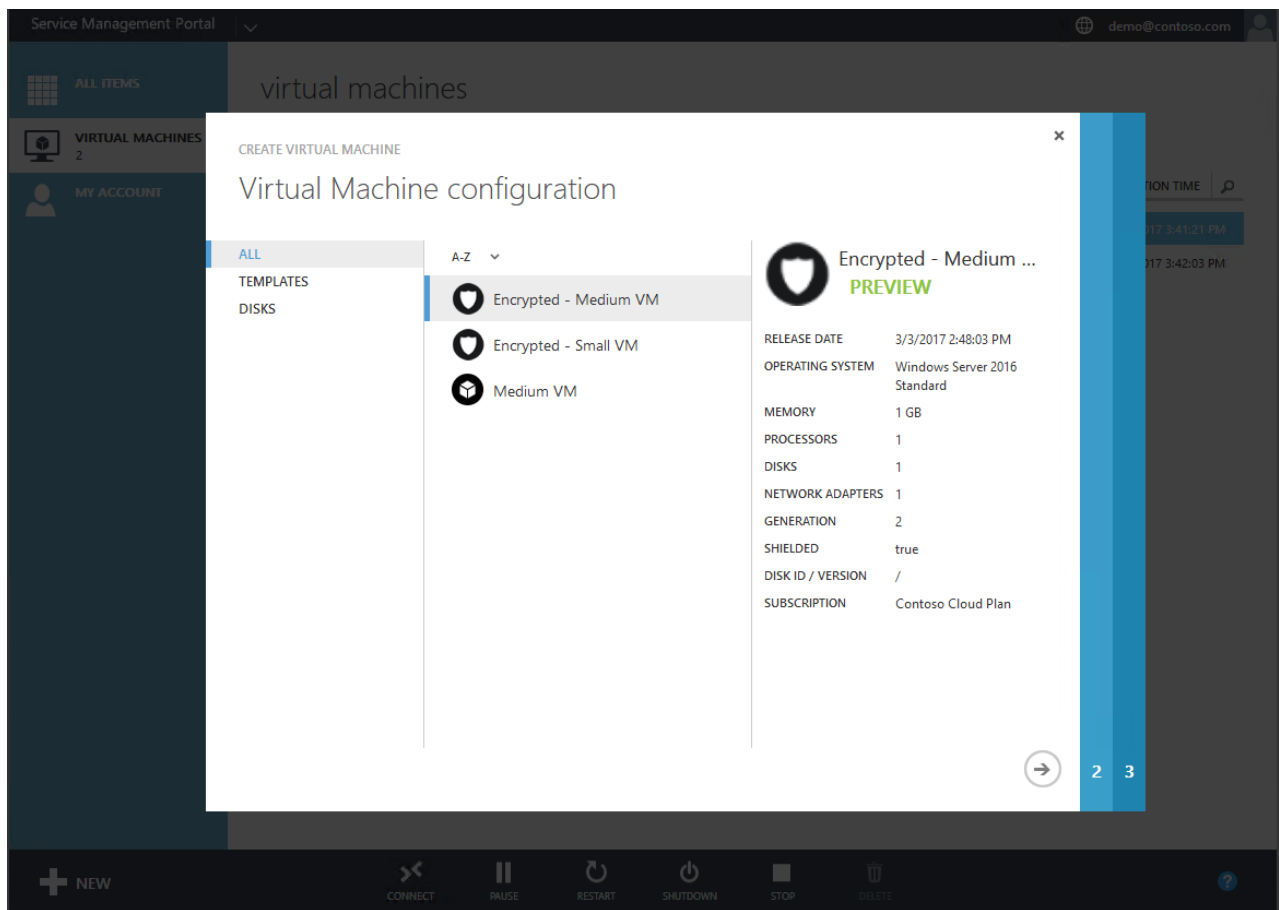
Ein kleineres Maß an Schutz, das immer noch die Kompatibilitäts Vorteile der Verschlüsselung eines virtuellen Computers bietet, aber Hyper-V-Administratoren die Verwendung von VM Console Connection und PowerShell Direct ermöglicht.

The screenshot shows the 'Shielding Data File Wizard' window. The title bar includes the Windows logo and the text 'Shielding Data File Wizard'. The window has standard Windows window controls (minimize, maximize, close). The main content area is titled 'File and Policy Selection'. On the left, there is a sidebar with a list of steps: 'File and Policy Selection' (highlighted in blue), 'Owner and Guardians', 'Volume ID Qualifiers', 'Specialization Values', 'Review Settings', 'Shielding Data File Gener...', and 'Summary'. The main area contains two radio button options: 'Import and edit an existing shielding data file' and 'Create a new shielding data file'. The 'Create a new shielding data file' option is selected. Below this, there is a text box for 'Shielding data file:' with a 'Browse' button. Further down, there are two radio button options for the type of shielding data: 'Shielding data for Shielded templates' (selected) and 'Shielding data for existing VMs and non-Shielded templates'. Below these, there is a section titled 'Virtual Machines that use this shielding data file will become:' with two radio button options: 'Shielded' (selected) and 'Encryption Supported'. The 'Shielded' option has a description: 'All security settings are enabled, including disk encryption, and cannot be reconfigured by Hyper-V administrators. Console access to the Virtual Machine is not permitted.' The 'Encryption Supported' option has a description: 'Supports disk encryption and permits Hyper-V administrators to configure other security settings as needed.' At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Generate', and 'Cancel'.

Sie können optionale Verwaltungs Elemente wie VMM oder Windows Azure Pack hinzufügen. Wenn Sie einen virtuellen Computer erstellen möchten, ohne diese Komponenten zu installieren, finden Sie weitere Informationen unter [Schritt für Schritt – Erstellen von abgeschirmten VMS ohne VMM](#).

Schritt 6: Erstellen einer abgeschirmten VM

Das Erstellen von abgeschirmten virtuellen Computern unterscheidet sich nur geringfügig von herkömmlichen virtuellen Computern. In Windows Azure Pack ist die-Funktion sogar noch einfacher als das Erstellen einer regulären VM, da Sie lediglich einen Namen, eine geschützte Datendatei (mit den restlichen Spezialisierungs Informationen) und das VM-Netzwerk angeben müssen.



Nächster Schritt

Voraussetzungen für HGS

Bereitstellen des Host-Überwachungs Diensts (HGS)

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Um die HGS bereitzustellen, führen Sie die folgenden Aufgaben aus:

- [Vorbereiten der Bereitstellung des Host-Überwachungs Diensts](#)
- [Installieren von HGS](#)
- [Initialisieren von HGS](#)
- [Konfigurieren von HTTPS \(optional\)](#)
- [Hinzufügen von Knoten](#)

Siehe auch

- [Bereitstellen des Host-Überwachungs Diensts für geschützte Hosts und abgeschirmte VMS](#)
- [Konfigurationsschritte für Hyper-V-Hosts, die zu überwachten Hosts werden](#)

Überprüfen der Voraussetzungen für den Host-Überwachungsdienst

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

In diesem Thema werden die Voraussetzungen für HGS und die ersten Schritte zur Vorbereitung der Bereitstellung von HGS behandelt.

Erforderliche Komponenten

- **Hardware:** HGS können auf physischen oder virtuellen Computern ausgeführt werden, es werden jedoch physische Computer empfohlen.

Wenn Sie HGS als physischen Cluster mit drei Knoten (für Verfügbarkeit) ausführen möchten, müssen Sie über drei physische Server verfügen. (Als bewährte Methode für das Clustering sollten die drei Server über eine sehr ähnliche Hardware verfügen.)

- **Betriebssystem:** für den Host Schlüssel Nachweis ist Windows Server 2019 Standard oder Datacenter Edition mit einem [v2](#)-Nachweis erforderlich. Bei einem TPM-basierten Nachweis können auf HGS Windows Server 2019 oder Windows Server 2016, Standard oder Datacenter Edition ausgeführt werden.
- **Server Rollen:** Host-Überwachungsdienst und unterstützende Server Rollen.
- **Konfigurations Berechtigungen/Berechtigungen für die Fabric-Domäne (Host) :** Sie müssen die DNS-Weiterleitung zwischen der Fabric-Domäne (Host) und der HGS-Domäne konfigurieren.

Aktualisieren von HGS

Wenn Sie bereits HGS bereitgestellt haben und ein Upgrade des Betriebssystems durchführen möchten, befolgen Sie die Anweisungen zum [Upgrade](#) , um Ihre HGS und Hyper-V-Server auf das neueste Betriebssystem zu aktualisieren.

Nächster Schritt

[Zertifikate für HGS abrufen](#)

Zertifikate für HGS abrufen

09.04.2020 • 7 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Beim Bereitstellen von HGS werden Sie aufgefordert, Signatur- und Verschlüsselungszertifikate bereitzustellen, die zum Schutz vertraulicher Informationen verwendet werden, die zum Starten einer abgesicherten VM benötigt werden. Diese Zertifikate verlassen niemals HGS und werden nur zum Entschlüsseln geschützter VM-Schlüssel verwendet, wenn der Host, auf dem Sie ausgeführt werden, bewiesen hat, dass Sie fehlerfrei ist. Mandanten (VM-Besitzer) verwenden die öffentliche Hälfte der Zertifikate, um Ihr Rechenzentrum zum Ausführen ihrer abgesicherten VMS zu autorisieren. In diesem Abschnitt werden die erforderlichen Schritte zum Abrufen kompatibler Signatur- und Verschlüsselungszertifikate für HGS behandelt.

Anfordern von Zertifikaten von Ihrer Zertifizierungsstelle

Es ist zwar nicht erforderlich, aber es wird dringend empfohlen, dass Sie Ihre Zertifikate von einer vertrauenswürdigen Zertifizierungsstelle abrufen. Auf diese Weise können die VM-Besitzer überprüfen, ob Sie den richtigen HGS-Server (d. h. Dienstanbieter oder Datacenter) zum Ausführen ihrer abgesicherten VMS autorisiert haben. In einem Unternehmensszenario können Sie Ihre eigene Unternehmenszertifizierungsstelle verwenden, um diese Zertifikate auszugeben. Host und Dienstanbieter sollten stattdessen eine bekannte öffentliche Zertifizierungsstelle verwenden.

Die Signatur- und Verschlüsselungszertifikate müssen mit den folgenden certificate-Eigenschaften ausgestellt werden (es sei denn, Sie sind als "empfohlen" gekennzeichnet):

ZERTIFIKAT VORLAGEN EIGENSCHAFT	ERFORDERLICHER WERT
Kryptografieanbieter	Alle Schlüsselspeicher-Anbieter (Key Storage Provider, KSP). Ältere Kryptografiedienstleister (CSPs) werden nicht unterstützt.
Schlüssel Algorithmus	RSA
Minimale Schlüsselgröße	2.048 Bits
Signatur Algorithmus	Empfohlen: SHA256
Schlüsselverwendung	Digitale Signatur <i>und</i> Datenverschlüsselung
Erweiterte Schlüsselverwendung	Serverauthentifizierung
Richtlinie zur Schlüssel Erneuerung	Erneuern Sie mit demselben Schlüssel. Durch das Erneuern von HGS-Zertifikaten mit unterschiedlichen Schlüsseln wird verhindert, dass abgesicherte VMS gestartet werden.
Antragstellername	Empfohlen: Name oder Webadresse Ihres Unternehmens. Diese Informationen werden den VM-Besitzern im Assistenten für die Schutzdatei angezeigt.

Diese Anforderungen gelten unabhängig davon, ob Sie Zertifikate verwenden, die von Hardware oder Software

unterstützt werden. Aus Sicherheitsgründen wird empfohlen, die HGS-Schlüssel in einem Hardware Sicherheitsmodul (HSM) zu erstellen, um zu verhindern, dass private Schlüssel vom System kopiert werden. Befolgen Sie die Anweisungen des HSM-Anbieters, um Zertifikate mit den obigen Attributen anzufordern, und installieren und autorisieren Sie den HSM-KSP auf jedem HGS-Knoten.

Jeder HGS-Knoten benötigt Zugriff auf dieselben Signatur- und Verschlüsselungszertifikate. Wenn Sie softwaregestützte Zertifikate verwenden, können Sie Ihre Zertifikate in eine PFX-Datei mit einem Kennwort exportieren und zulassen, dass HGS die Zertifikate für Sie verwaltet. Sie haben auch die Möglichkeit, die Zertifikate im Zertifikat-Speicher des lokalen Computers auf jedem HGS-Knoten zu installieren und den Fingerabdruck für HGS bereitzustellen. Beide Optionen werden im Thema [Initialisieren des HGS-Clusters](#) erläutert.

Erstellen selbst signierter Zertifikate für Testszenarien

Wenn Sie eine HGS-Lab-Umgebung erstellen und nicht über eine Zertifizierungsstelle verfügen oder diese verwenden möchten, können Sie selbst signierte Zertifikate erstellen. Beim Importieren der Zertifikatsinformationen im Assistenten für Schutz Datendateien wird eine Warnung angezeigt, aber alle Funktionen bleiben unverändert.

Führen Sie die folgenden Befehle in PowerShell aus, um selbst signierte Zertifikate zu erstellen und in eine PFX-Datei zu exportieren:

```
$certificatePassword = Read-Host -AsSecureString -Prompt "Enter a password for the PFX file"

$signCert = New-SelfSignedCertificate -Subject "CN=HGS Signing Certificate"
Export-PfxCertificate -FilePath .\signCert.pfx -Password $certificatePassword -Cert $signCert
Remove-Item $signCert.PSPath

$encCert = New-SelfSignedCertificate -Subject "CN=HGS Encryption Certificate"
Export-PfxCertificate -FilePath .\encCert.pfx -Password $certificatePassword -Cert $encCert
Remove-Item $encCert.PSPath
```

Anfordern eines SSL-Zertifikats

Alle Schlüssel und vertraulichen Informationen, die zwischen Hyper-V-Hosts und HGS übertragen werden, werden auf der Nachrichten-Ebene verschlüsselt, d. h., die Informationen werden mit Schlüsseln verschlüsselt, die HGS oder Hyper-v genannt werden. Dadurch wird verhindert, dass ein Benutzer den Netzwerk-Datenverkehr ausfängt und Schlüssel für Ihre VMS stiehlt. Wenn Sie jedoch Kompatibilitätsanforderungen haben oder einfach die gesamte Kommunikation zwischen Hyper-V und HGS verschlüsseln möchten, können Sie HGS mit einem SSL-Zertifikat konfigurieren, mit dem alle Daten auf der Transport-Ebene verschlüsselt werden.

Die Hyper-V-Hosts und HGS-Knoten müssen das von Ihnen bereitgestellte SSL-Zertifikat als vertrauenswürdig einstufen. Daher wird empfohlen, dass Sie das SSL-Zertifikat von Ihrer Unternehmens-Zertifizierungsstelle anfordern. Wenn Sie das Zertifikat anfordern, müssen Sie Folgendes angeben:

SSL-ZERTIFIKAT EIGENSCHAFT	ERFORDERLICHER WERT
Antragstellername	Der Name des HGS-Clusters (als Name des verteilten Netzwerks oder des FQDN des virtuellen Computer Objekts bezeichnet). Dabei handelt es sich um die Verkettung Ihres HGS-Dienstnamens, der für <code>Initialize-HgsServer</code> und ihren HGS-Domänen Namen angegeben wird.
Alternativer Antragsteller Name	Wenn Sie einen anderen DNS-Namen verwenden, um Ihren HGS-Cluster zu erreichen (z. B. wenn er sich hinter einem Load Balancer befindet), müssen Sie diese DNS-Namen in das Feld San ihrer Zertifikat Anforderung einschließen.

Die Optionen zum Angeben dieses Zertifikats beim Initialisieren des HGS-Servers finden Sie unter [Konfigurieren des ersten HGS-Knotens](#). Sie können das SSL-Zertifikat auch zu einem späteren Zeitpunkt mit dem Cmdlet [Set-hgsserver](#) hinzufügen oder ändern.

Nächster Schritt

[Installieren von HGS](#)

Wählen Sie aus, ob HGS in einer eigenen dedizierten Gesamtstruktur oder in einer vorhandenen geschützten Gesamtstruktur installiert werden.

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Die Active Directory-Gesamtstruktur für HGS ist sensibel, da die Administratoren Zugriff auf die Schlüssel haben, mit denen abgeschirmte VMS gesteuert werden. Bei der Standardinstallation wird eine neue, für HGS dedizierte Gesamtstruktur eingerichtet und andere Abhängigkeiten konfiguriert. Diese Option wird empfohlen, da die Umgebung eigenständig ist und bekanntermaßen sicher ist, wenn Sie erstellt wird.

Die einzige Technische Voraussetzung für die Installation von HGS in einer vorhandenen Gesamtstruktur ist, dass Sie der Stamm Domäne hinzugefügt wird. nicht-Stamm Domänen werden nicht unterstützt. Es gibt aber auch Betriebsanforderungen und sicherheitsrelevante bewährte Methoden für die Verwendung einer vorhandenen Gesamtstruktur. Geeignete Gesamtstrukturen werden absichtlich erstellt, um eine sensible Funktion zu erfüllen, z. b. die Gesamtstruktur, die von [privileged Access Management für AD DS](#) oder eine [Erweiterte Sicherheits Verwaltungs Umgebung \(ESAE\)](#) verwendet wird. Diese Gesamtstrukturen weisen in der Regel die folgenden Merkmale auf:

- Sie haben nur wenige Administratoren (getrennt von Fabric-Administratoren).
- Sie verfügen über eine geringe Anzahl von Anmeldungen.
- Dabei handelt es sich nicht um allgemeine Zwecke.

Allgemeine Gesamtstrukturen, wie z. b. Produktions Gesamtstrukturen, sind nicht für die Verwendung durch HGS geeignet. Fabric-Gesamtstrukturen sind auch ungeeignet, da HGS von fabricadministratoren isoliert werden müssen.

Nächster Schritt

Wählen Sie die Installationsoption, die für Ihre Umgebung am besten geeignet ist:

- [Installieren von HGS in einer eigenen dedizierten Gesamtstruktur](#)
- [Installieren von HGS in einer vorhandenen geschützten Gesamtstruktur](#)

Installieren von HGS in einer neuen Gesamtstruktur

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Hinzufügen der HGS-Server Rolle

Führen Sie die folgenden Befehle in einer PowerShell-Sitzung mit erhöhten Rechten aus, um die HGS-Server Rolle hinzufügen und HGS installieren.

Fügen Sie die Host-Überwachungsdienst-Rolle mithilfe des folgenden Befehls hinzu:

```
Install-WindowsFeature -Name HostGuardianServiceRole -IncludeManagementTools -Restart
```

Installieren von HGS

Host-Überwachungsdienst sollte in einer separaten Active Directory-Gesamtstruktur installiert werden. Stellen Sie sicher, dass der Host-Überwachungsdienst Computer **nicht** in eine Domäne eingebunden werden, bevor Sie beginnen, und melden Sie sich als dem lokalen Computer-vorerst.

Führen Sie die folgenden Befehle zum Host-Überwachungsdienst installieren und Konfigurieren der Domäne. Das Kennwort, die hier angegebenen gilt nur für Active Directory in das Verzeichnisdienst-Wiederherstellungsmodus Kennwort; Es wird *nicht* Anmeldekennwort für Ihr Administratorkonto ändern. Sie können jeden Domänennamen Ihrer Wahl für die-HgsDomainName bereitstellen.

```
$adminPassword = ConvertTo-SecureString -AsPlainText '<password>' -Force  
  
Install-HgsServer -HgsDomainName 'bastion.local' -SafeModeAdministratorPassword $adminPassword -Restart
```

Nächste Schritte

- Die nächsten Schritte zum Einrichten eines TPM-basierten Nachweis finden Sie unter [Initialisieren des HGS-Clusters mit dem TPM-Modus in einer neuen dedizierten Gesamtstruktur \(Standard\)](#).
- Die nächsten Schritte zum Einrichten des Host Schlüssel-Attestation finden Sie unter [Initialisieren des HGS-Clusters mithilfe des Schlüssel Modus in einer neuen dedizierten Gesamtstruktur \(Standard\)](#).
- Die nächsten Schritte zum Einrichten des Administrator basierten Nachweis (veraltet in Windows Server 2019) finden Sie unter [Initialisieren des HGS-Clusters mit dem AD-Modus in einer neuen dedizierten Gesamtstruktur \(Standard\)](#).

Nächster Schritt

[Initialisieren von HGS](#)

Installieren von HGS in einer vorhandenen geschützten Gesamtstruktur

09.04.2020 • 9 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Fügen Sie den HGS-Server der vorhandenen Domäne hinzu.

In einer vorhandenen geschützten Gesamtstruktur müssen HGS der Stamm Domäne hinzugefügt werden. Verwenden Sie Server-Manager oder [Add-Computer](#) , um den HGS-Server mit der Stamm Domäne zu verknüpfen.

Hinzufügen der HGS-Server Rolle

Führen Sie alle Befehle in diesem Thema in einer PowerShell-Sitzung mit erhöhten Rechten aus.

Fügen Sie die Host-Überwachungsdienst-Rolle mithilfe des folgenden Befehls hinzu:

```
Install-WindowsFeature -Name HostGuardianServiceRole -IncludeManagementTools -Restart
```

Wenn Ihr Rechenzentrum über eine sichere geschützte Gesamtstruktur verfügt, der Sie HGS-Knoten beitreten möchten, führen Sie die folgenden Schritte aus. Sie können diese Schritte auch verwenden, um zwei oder mehr unabhängige HGS-Cluster zu konfigurieren, die mit derselben Domäne verknüpft sind.

Fügen Sie den HGS-Server der vorhandenen Domäne hinzu.

Verwenden Sie Server-Manager oder [Add-Computer](#) , um die HGS-Server mit der gewünschten Domäne zu verknüpfen.

Vorbereiten von Active Directory Objekten

Erstellen Sie ein Gruppen verwaltetes Dienst Konto und zwei Sicherheitsgruppen. Sie können die Cluster Objekte auch vorab bereitstellen, wenn das Konto, mit dem Sie HGS initialisieren, nicht über die Berechtigung zum Erstellen von Computer Objekten in der Domäne verfügt.

Gruppen verwaltetes Dienst Konto

Das Gruppen verwaltete Dienst Konto (Group Managed Service Account, GMSA) ist die Identität, die von HGS zum Abrufen und Verwenden der Zertifikate verwendet wird. Verwenden Sie [New-ADServiceAccount](#) , um ein GMSA zu erstellen. Wenn dies das erste GMSA in der Domäne ist, müssen Sie einen Schlüssel Verteilungsdienst-Stamm Schlüssel hinzufügen.

Jedem HGS-Knoten muss der Zugriff auf das GMSA-Kennwort gestattet werden. Die einfachste Möglichkeit, dies zu konfigurieren, besteht darin, eine Sicherheitsgruppe zu erstellen, die alle Ihre HGS-Knoten enthält, und dieser Sicherheitsgruppe Zugriff zu gewähren, um das GMSA-Kennwort abzurufen.

Sie müssen den HGS-Server neu starten, nachdem Sie ihn einer Sicherheitsgruppe hinzugefügt haben, um sicherzustellen, dass er die neue Gruppenmitgliedschaft erhält.

```
# Check if the KDS root key has been set up
if (-not (Get-KdsRootKey)) {
    # Adds a KDS root key effective immediately (ignores normal 10 hour waiting period)
    Add-KdsRootKey -EffectiveTime ((Get-Date).AddHours(-10))
}

# Create a security group for HGS nodes
$hgsNodes = New-ADGroup -Name 'HgsServers' -GroupScope DomainLocal -PassThru

# Add your HGS nodes to this group
# If your HGS server object is under an organizational unit, provide the full distinguished name instead of
"HGS01"
Add-ADGroupMember -Identity $hgsNodes -Members "HGS01"

# Create the gMSA
New-ADServiceAccount -Name 'HGSgMSA' -DnsHostName 'HGSgMSA.yourdomain.com' -
PrincipalsAllowedToRetrieveManagedPassword $hgsNodes
```

Das GMSA benötigt das Recht, Ereignisse im Sicherheitsprotokoll auf jedem HGS-Server zu generieren. Wenn Sie Gruppenrichtlinie verwenden, um die Zuweisung von Benutzerrechten zu konfigurieren, stellen Sie sicher, dass dem GMSA-Konto die [Berechtigung Audit-Ereignisse generieren](#) auf Ihren HGS-Servern erteilt wird.

NOTE

Gruppen verwaltete Dienst Konten sind ab dem Windows Server 2012-Active Directory Schema verfügbar. Weitere Informationen finden Sie unter [Gruppen verwaltete Dienst Kontoanforderungen](#).

Jea-Sicherheitsgruppen

Wenn Sie HGS einrichten, wird ein Jea-PowerShell-Endpunkt ([Just Enough Administration](#)) konfiguriert, um Administratoren das Verwalten von HGS ohne volle lokale Administratorrechte zu ermöglichen. Sie müssen Jea nicht zum Verwalten von HGS verwenden, aber es muss beim Ausführen von Initialize-hgsserver weiterhin konfiguriert werden. Die Konfiguration des Jea-Endpunkts besteht aus dem Festlegen von zwei Sicherheitsgruppen, die ihre HGS-Administratoren und HGS-Reviewer enthalten. Benutzer, die der Administrator Gruppe angehören, können Richtlinien auf HGS hinzufügen, ändern oder entfernen. Reviewer können die aktuelle Konfiguration nur anzeigen.

Erstellen Sie zwei Sicherheitsgruppen für diese Jea-Gruppen, indem Sie Active Directory Admin Tools oder [New-adgroup](#) verwenden.

```
New-ADGroup -Name 'HgsJeaReviewers' -GroupScope DomainLocal
New-ADGroup -Name 'HgsJeaAdmins' -GroupScope DomainLocal
```

Cluster Objekte

Wenn das Konto, das Sie zum Einrichten von HGS verwenden, nicht über die Berechtigung zum Erstellen neuer Computer Objekte in der Domäne verfügt, müssen Sie die Cluster Objekte vorab bereitstellen. Diese Schritte werden unter vorab Bereitstellen von [Cluster Computer Objekten in Active Directory Domain Services](#) erläutert.

Zum Einrichten des ersten HGS-Knotens müssen Sie ein Cluster Namen Objekt (CNO) und ein virtuelles Computer Objekt (VCO) erstellen. Das CNO stellt den Namen des Clusters dar und wird hauptsächlich intern vom Failoverclustering verwendet. VCO stellt den HGS-Dienst dar, der sich auf dem Cluster befindet, und ist der Name, der beim DNS-Server registriert ist.

IMPORTANT

Der Benutzer, der `Initialize-HgsServer` ausführen wird, muss die **vollständige Kontrolle** über die CNO- und VCO-Objekte in Active Directory haben.

Wenn Sie CNO und VCO schnell vorab bereitstellen möchten, müssen Sie über einen Active Directory Administrator die folgenden PowerShell-Befehle ausführen:

```
# Create the CNO
$cno = New-ADComputer -Name 'HgsCluster' -Description 'HGS CNO' -Enabled $false -Passthru

# Create the VCO
$vco = New-ADComputer -Name 'HgsService' -Description 'HGS VCO' -Passthru

# Give the CNO full control over the VCO
$vcoPath = Join-Path "AD:\" $vco.DistinguishedName
$acl = Get-Acl $vcoPath
$ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule $cno.SID, "GenericAll", "Allow"
$acl.AddAccessRule($ace)
Set-Acl -Path $vcoPath -AclObject $acl

# Allow time for your new CNO and VCO to replicate to your other Domain Controllers before continuing
```

Sicherheitsbaseline-Ausnahmen

Wenn Sie HGS in einer stark gesperrten Umgebung bereitstellen, können bestimmte Gruppenrichtlinie-Einstellungen verhindern, dass HGS ordnungsgemäß funktionieren. Überprüfen Sie die Gruppenrichtlinie-Objekte auf die folgenden Einstellungen, und befolgen Sie die Anweisungen, wenn Sie betroffen sind:

Netzwerk Anmeldung

Richtlinien Pfad: Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Zuweisen von Benutzerrechten

Richtlinien Name: Zugriff vom Netzwerk auf diesen Computer verweigern

Erforderlicher Wert: Stellen Sie sicher, dass der Wert keine Netzwerk Anmeldungen für alle lokalen Konten blockiert. Lokale Administrator Konten können jedoch problemlos blockiert werden.

Grund: Failoverclustering basiert auf einem lokalen Konto mit dem Namen clusr, das nicht Administrator ist, um Cluster Knoten zu verwalten. Durch das Blockieren der Netzwerk Anmeldung für diesen Benutzer wird verhindert, dass der Cluster ordnungsgemäß funktioniert.

Kerberos-Verschlüsselung

Richtlinien Pfad: Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen

Richtlinien Name: Netzwerksicherheit: Konfigurieren der für Kerberos zulässigen Verschlüsselungstypen

Aktion: Wenn diese Richtlinie konfiguriert ist, müssen Sie das GMSA-Konto mit "[Set-ADServiceAccount](#)" aktualisieren, sodass nur die unterstützten Verschlüsselungstypen in dieser Richtlinie verwendet werden. Wenn Ihre Richtlinie beispielsweise nur AES128_HMAC_SHA1 und AES256_HMAC_SHA1 zulässt, sollten Sie

```
Set-ADServiceAccount -Identity HGSgMSA -KerberosEncryptionType AES128,AES256
```

 ausführen.

Nächste Schritte

- Die nächsten Schritte zum Einrichten eines TPM-basierten Nachweis finden Sie unter [Initialisieren des HGS-Clusters mit dem TPM-Modus in einer vorhandenen](#) geschützten Gesamtstruktur.

- Die nächsten Schritte zum Einrichten des Host Schlüssel-Attestation finden Sie unter [Initialisieren des HGS-Clusters mithilfe des Schlüssel Modus in einer vorhandenen](#)geschützten Gesamtstruktur.
- Die nächsten Schritte zum Einrichten des Administrator basierten Nachweis (in Windows Server 2019 veraltet) finden Sie unter [Initialisieren des HGS-Clusters mit dem AD-Modus in einer vorhandenen](#)geschützten Gesamtstruktur.

Initialisieren des Host-Überwachungs Diensts (HGS)

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Wenn Sie HGS initialisieren, geben Sie den Modus an, der von HGS zum Messen der Integrität der überwachten Hosts verwendet wird. Es gibt zwei Optionen, die sich gegenseitig ausschließen. Hintergrundinformationen zum ausgewählten Modus finden Sie im [Planungs Handbuch für geschützte Fabric und abgeschirmte VMs für Hoster](#).

In den folgenden Themen werden die Bereitstellungs Schritte für die einzelnen Modi behandelt:

- [TPM-vertrauenswürdiger Nachweis \(TPM-Modus\)](#)
- [Host Schlüssel Nachweis \(Schlüssel Modus\)](#)
- [Admin-vertrauenswürdiger Nachweis \(AD-Modus\)](#)

Sie sollten diese Schritte auf einem physischen Server ausführen.

Initialisieren von HGS mithilfe von TPM-vertrauenswürdigem Nachweis

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Diese Schritte sind abhängig davon, ob Sie HGS in einer neuen Gesamtstruktur oder in einer vorhandenen geschützten Gesamtstruktur initialisieren:

1. [Initialisieren des HGS-Clusters in einer neuen Gesamtstruktur \(Standard\)](#)

– Oder –

[Initialisieren des HGS-Clusters in einer vorhandenen geschützten Gesamtstruktur](#)

2. [Installieren Sie vertrauenswürdige TPM-Stamm Zertifikate.](#)

3. [Konfigurieren des Fabric-DNS](#)

Initialisieren des HGS-Clusters mit dem TPM-Modus in einer neuen dedizierten Gesamtstruktur (Standard)

09.04.2020 • 5 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

1. Clients können einen beliebigen Knoten des Host-Überwachungsdienst mit Failover-Clusterunterstützung verteilten Netzwerknamen (DNN) problemlos kontaktieren. Sie müssen ein DNN auswählen. Dieser Name wird in den HGS DNS-Dienst registriert werden. Beispielsweise können bei 3 HGS-Knoten mit Hostnamen HGS01 HGS02 und HGS03, möglicherweise möchten Sie "Host-Überwachungsdienst" oder "HgsCluster" für das DNN auswählen.
2. Suchen Sie Ihr HGS-Überwachungsdienst-Zertifikate. Sie benötigen ein Signaturzertifikat und ein Verschlüsselungszertifikat clientkonfigurationsobjekt des Host-Überwachungsdienst-Clusters. Die einfachste Möglichkeit zum Angeben der Zertifikate auf dem Host-Überwachungsdienst ist eine kennwortgeschützte PFX-Datei für jedes Zertifikat zu erstellen, die die öffentlichen und privaten Schlüssel enthält. Wenn Sie HSM-gesicherten Schlüsseln oder andere nicht exportierbare Zertifikate verwenden, stellen Sie sicher, dass das Zertifikat in den Zertifikatspeicher des lokalen Computers installiert ist, bevor Sie fortfahren. Weitere Informationen, welche Zertifikate verwenden können, finden Sie unter [Abrufen von Zertifikaten für die Host-Überwachungsdienst](#).
3. Führen Sie [Initialize-hgsserver](#) in einem PowerShell-Fenster mit erhöhten Rechten auf dem ersten HGS-Knoten aus. Die Syntax dieses Cmdlets unterstützt viele verschiedene Eingaben, aber die zwei häufigsten Aufrufe sind unten aufgeführt:

- Wenn Sie PFX-Dateien für Ihre Signatur- und Verschlüsselungszertifikate verwenden, führen Sie die folgenden Befehle aus:

```
$signingCertPass = Read-Host -AsSecureString -Prompt "Signing certificate password"
$encryptionCertPass = Read-Host -AsSecureString -Prompt "Encryption certificate password"

Initialize-HgsServer -HgsServiceName 'MyHgsDNN' -SigningCertificatePath '.\signCert.pfx' -
SigningCertificatePassword $signingCertPass -EncryptionCertificatePath '.\encCert.pfx' -
EncryptionCertificatePassword $encryptionCertPass -TrustTpm
```

- Wenn Sie nicht exportierbare Zertifikate verwenden, die im lokalen Zertifikat Speicher installiert sind, führen Sie den folgenden Befehl aus. Wenn Sie die Fingerabdrücke ihrer Zertifikate nicht kennen, können Sie die verfügbaren Zertifikate auflisten, indem Sie `Get-ChildItem Cert:\LocalMachine\My` ausführen.

```
Initialize-HgsServer -HgsServiceName 'MyHgsDNN' -SigningCertificateThumbprint '1A2B3C4D5E6F...' -
EncryptionCertificateThumbprint '0F9E8D7C6B5A...' -TrustTpm
```

4. Wenn Sie Zertifikate für Host-Überwachungsdienst Fingerabdrücke verwenden bereitgestellt, werden Sie aufgefordert, Host-Überwachungsdienst Zugriff auf den privaten Schlüssel dieser Zertifikate gewährt werden. Führen Sie auf einem Server mit Desktopdarstellung, die installiert werden soll die folgenden Schritte aus:
 - a. Öffnen Sie den Zertifikat-Manager für lokalen Computer ("certlm.msc")
 - b. Suchen Sie die Zertifikate > mit der rechten Maustaste > alle Aufgaben > Privatschlüssel verwalten

- c. Klicken Sie auf **Hinzufügen**.
 - d. Klicken Sie im Auswahlfenster Objekt auf **Objekttypen** , und aktivieren Sie **-Dienstkonten**
 - e. Geben Sie den Namen des Dienstkontos erwähnt in den Text der Warnung aus `Initialize-HgsServer`
 - f. Stellen Sie sicher, dass das gruppenverwaltete Dienstkonto "Lesen" für den privaten Schlüssel zugreifen.
- Auf Server Core aufweist müssen Sie ein PowerShell-Modul zur Unterstützung bei der Festlegung der Berechtigungen für den privaten Schlüssel herunterladen.

- a. Führen Sie `Install-Module GuardedFabricTools` auf dem Server-Host-Überwachungsdienst, verfügt er über Internetkonnektivität, oder führen Sie `Save-Module GuardedFabricTools` auf einem anderen Computer und kopieren Sie das Modul über den HGS-Server.
- b. Führen Sie `Import-Module GuardedFabricTools` aus. Dadurch wird zusätzliche Eigenschaften finden Sie in PowerShell zertifikatobjekten hinzugefügt.
- c. Suchen Sie den Zertifikatfingerabdruck in PowerShell mit `Get-ChildItem Cert:\LocalMachine\My`
- d. Aktualisieren Sie die ACL, und Ersetzen Sie dabei den Fingerabdruck durch Ihre eigenen und das gMSA-Konto mit dem Konto in den folgenden Code im Warnungstext aufgeführt
`Initialize-HgsServer` .

```
$certificate = Get-Item "Cert:\LocalMachine\1A2B3C..."  
$certificate.Acl = $certificate.Acl | Add-AccessRule "HgsSvc_1A2B3C" Read Allow
```

Wenn Sie HSM-gesicherten Zertifikate verwenden, oder die Zertifikate, in gespeichert von Drittanbietern Key Storage Provider, diese Schritte gelten möglicherweise nicht für Sie. Dokumentation des Schlüsselspeicheranbieters für die Informationen zum Verwalten von Berechtigungen für Ihren privaten Schlüssel. In einigen Fällen steht keine Autorisierung oder Autorisierung wird für den gesamten Computer bereitgestellt, wenn das Zertifikat installiert ist.

- 5. Das ist alles! In einer Produktionsumgebung sollten Sie weiterhin [zusätzliche HGS-Knoten zu Ihrem Cluster hinzufügen](#).

Nächster Schritt

[Installieren von TPM-Stammzertifikaten](#)

Initialisieren des HGS-Clusters mit dem TPM-Modus in einer vorhandenen geschützten Gesamtstruktur

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Active Directory Domain Services wird auf dem Computer installiert, sollte jedoch nicht konfiguriert bleiben.

Suchen Sie Ihr HGS-Überwachungsdienst-Zertifikate. Sie benötigen ein Signaturzertifikat und ein Verschlüsselungszertifikat clientkonfigurationsobjekt des Host-Überwachungsdienst-Clusters. Die einfachste Möglichkeit zum Angeben der Zertifikate auf dem Host-Überwachungsdienst ist eine kennwortgeschützte PFX-Datei für jedes Zertifikat zu erstellen, die die öffentlichen und privaten Schlüssel enthält. Wenn Sie HSM-gesicherten Schlüsseln oder andere nicht exportierbare Zertifikate verwenden, stellen Sie sicher, dass das Zertifikat in den Zertifikatspeicher des lokalen Computers installiert ist, bevor Sie fortfahren. Weitere Informationen, welche Zertifikate verwenden können, finden Sie unter [Abrufen von Zertifikaten für die Host-Überwachungsdienst](#).

Bevor Sie fortfahren, stellen Sie sicher, dass Sie die Cluster Objekte für den Host-Überwachungsdienst vorab bereitgestellt haben, und gewähren Sie dem angemeldeten Benutzer die **vollständige Kontrolle** über die VCO- und CNO-Objekte in Active Directory. Der Name des virtuellen Computer Objekts muss an den `-HgsServiceName` -Parameter übergeben werden, und der Cluster Name muss an den `-ClusterName` -Parameter übergeben werden.

TIP

Überprüfen Sie die AD-Domänen Controller, um sicherzustellen, dass Ihre Cluster Objekte auf alle DCS repliziert wurden

Wenn Sie PFX-basierte Zertifikate verwenden, führen Sie auf dem HGS-Server die folgenden Befehle aus:

```
$signingCertPass = Read-Host -AsSecureString -Prompt "Signing certificate password"
$encryptionCertPass = Read-Host -AsSecureString -Prompt "Encryption certificate password"

Install-ADServiceAccount -Identity 'HGSgMSA'

Initialize-HgsServer -UseExistingDomain -ServiceAccount 'HGSgMSA' -JeaReviewersGroup 'HgsJeaReviewers' -
JeaAdministratorsGroup 'HgsJeaAdmins' -HgsServiceName 'HgsService' -SigningCertificatePath '.\signCert.pfx' -
SigningCertificatePassword $signPass -EncryptionCertificatePath '.\encCert.pfx' -EncryptionCertificatePassword
$encryptionCertPass -TrustTpm
```

Wenn Sie Zertifikate verwenden, die auf dem lokalen Computer installiert sind (z. b. HSM-gestützte Zertifikate und nicht exportierbare Zertifikate), verwenden Sie stattdessen die Parameter "`-SigningCertificateThumbprint`" und "`-EncryptionCertificateThumbprint`".

Nächster Schritt

[Installieren von TPM-Stammzertifikaten](#)

Installieren Sie vertrauenswürdige TPM-Stamm Zertifikate.

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Wenn Sie HGS für die Verwendung des TPM-Attestation konfigurieren, müssen Sie auch HGS so konfigurieren, dass Sie den Anbietern der TPMs auf Ihren Servern vertrauen. Durch diesen zusätzlichen Überprüfungsprozess wird sichergestellt, dass nur echte vertrauenswürdige TPMs ihre HGS überzeugen können. Wenn Sie versuchen, ein nicht vertrauenswürdiges TPM bei `Add-HgsAttestationTpmHost` zu registrieren, erhalten Sie eine Fehlermeldung, die darauf hinweist, dass der TPM-Anbieter nicht vertrauenswürdig ist.

Um den TPMs zu vertrauen, müssen die Stamm- und zwischen Signatur Zertifikate, die zum Signieren des Endorsement Key in den TPMs Ihres Servers verwendet werden, auf HGS installiert werden. Wenn Sie in Ihrem Daten Center mehr als ein TPM-Modell verwenden, müssen Sie möglicherweise verschiedene Zertifikate für jedes Modell installieren. HGS sehen sich die Zertifikat Speicher "TrustedTPM_RootCA" und "TrustedTPM_IntermediateCA" für die herstellerzertifikate an.

NOTE

Die TPM-herstellerzertifikate unterscheiden sich von den standardmäßig in Windows installierten Stamm- und zwischen Zertifikaten, die von TPM-Anbietern verwendet werden.

Eine Sammlung vertrauenswürdiger TPM-Stamm- und zwischen Zertifikate wird von Microsoft zur einfacheren Veröffentlichung veröffentlicht. Mithilfe der nachfolgenden Schritte können Sie diese Zertifikate installieren. Wenn Ihre TPM-Zertifikate nicht im folgenden Paket enthalten sind, wenden Sie sich an den TPM-Hersteller oder den OEM-Server, um die Stamm- und zwischen Zertifikate für ihr bestimmtes TPM-Modell zu erhalten.

Wiederholen Sie die folgenden Schritte auf **jedem HGS-Server**:

1. Laden Sie das neueste Paket aus <https://go.microsoft.com/fwlink/?linkid=2097925> herunter.
2. Überprüfen Sie die Signatur der CAB-Datei, um ihre Echtheit sicherzustellen. Fahren Sie nicht fort, wenn die Signatur ungültig ist.

```
Get-AuthenticodeSignature .\TrustedTpm.cab
```

Ausgabebeispiel:

```
Directory: C:\Users\Administrator\Downloads
```

SignerCertificate	Status	Path
-----	-----	----
0DD6D4D4F46C0C7C2671962C4D361D607E370940	Valid	TrustedTpm.cab

3. Erweitern Sie die CAB-Datei.

```
mkdir .\TrustedTPM  
expand.exe -F:* <Path-To-TrustedTpm.cab> .\TrustedTPM
```

4. Standardmäßig installiert das Konfigurationsskript Zertifikate für jeden TPM-Anbieter. Wenn Sie nur Zertifikate für Ihren spezifischen TPM-Hersteller importieren möchten, löschen Sie die Ordner für TPM-Anbieter, die von Ihrer Organisation nicht als vertrauenswürdig eingestuft werden.
5. Installieren Sie das vertrauenswürdige Zertifikat Paket durch Ausführen des Setup Skripts im erweiterten Ordner.

```
cd .\TrustedTPM  
.\setup.cmd
```

Wenn Sie neue Zertifikate hinzufügen oder diese bei einer früheren Installation absichtlich übersprungen haben, wiederholen Sie einfach die oben beschriebenen Schritte auf jedem Knoten in Ihrem HGS-Cluster. Vorhandene Zertifikate bleiben vertrauenswürdig, aber der vertrauenswürdigen TPM-Speicher werden neue Zertifikate in der erweiterten CAB-Datei hinzugefügt.

Nächster Schritt

[Konfigurieren des Fabric-DNS](#)

Nächster Schritt

13.05.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Es gibt viele Möglichkeiten zum Konfigurieren der Namensauflösung für die Fabric-Domäne. Eine einfache Möglichkeit besteht darin, eine bedingte Weiterleitung-Zone im DNS für das Fabric zu einrichten. Führen Sie die folgenden Befehle zum Einrichten dieser Zone in einer Windows PowerShell-Konsole mit erhöhten Rechten auf einem Fabric-DNS-Server. Ersetzen Sie den Namen und Adressen in der Windows PowerShell-Syntax finden Sie unten nach Bedarf für Ihre Umgebung. Fügen Sie der Masterserver für die zusätzlichen HGS-Knoten hinzu.

```
Add-DnsServerConditionalForwarderZone -Name 'bastion.local' -ReplicationScope "Forest" -MasterServers <IP addresses of HGS server>
```

[Konfigurieren von HTTPS](#)

Siehe auch

- [Konfigurationsschritte für Hyper-V-Hosts, die als geschützte Hosts verwendet werden sollen](#)
- [Bereitstellungs Aufgaben für geschützte Fabrics und abgeschirmte VMS](#)

Initialisieren von HGS mithilfe des Host Schlüssel-Nachweis

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019

Dieser Schritt hängt davon ab, ob Sie HGS in einer neuen Gesamtstruktur oder in einer vorhandenen geschützten Gesamtstruktur initialisieren:

- [Initialisieren des HGS-Clusters in einer neuen Gesamtstruktur \(Standard\)](#)
 - Oder –
- [Initialisieren des HGS-Clusters in einer vorhandenen geschützten Gesamtstruktur](#)

Initialisieren des HGS-Clusters mithilfe des Schlüssel Modus in einer neuen dedizierten Gesamtstruktur (Standard)

09.04.2020 • 5 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2019, Windows Server 2016

1. Clients können einen beliebigen Knoten des Host-Überwachungsdienst mit Failover-Clusterunterstützung verteilten Netzwerknamen (DNN) problemlos kontaktieren. Sie müssen ein DNN auswählen. Dieser Name wird in den HGS DNS-Dienst registriert werden. Beispielsweise können bei 3 HGS-Knoten mit Hostnamen HGS01 HGS02 und HGS03, möglicherweise möchten Sie "Host-Überwachungsdienst" oder "HgsCluster" für das DNN auswählen.
2. Suchen Sie Ihr HGS-Überwachungsdienst-Zertifikate. Sie benötigen ein Signaturzertifikat und ein Verschlüsselungszertifikat clientkonfigurationsobjekt des Host-Überwachungsdienst-Clusters. Die einfachste Möglichkeit zum Angeben der Zertifikate auf dem Host-Überwachungsdienst ist eine kennwortgeschützte PFX-Datei für jedes Zertifikat zu erstellen, die die öffentlichen und privaten Schlüssel enthält. Wenn Sie HSM-gesicherten Schlüsseln oder andere nicht exportierbare Zertifikate verwenden, stellen Sie sicher, dass das Zertifikat in den Zertifikatspeicher des lokalen Computers installiert ist, bevor Sie fortfahren. Weitere Informationen, welche Zertifikate verwenden können, finden Sie unter [Abrufen von Zertifikaten für die Host-Überwachungsdienst](#).
3. Führen Sie [Initialize-hgsserver](#) in einem PowerShell-Fenster mit erhöhten Rechten auf dem ersten HGS-Knoten aus. Die Syntax dieses Cmdlets unterstützt viele verschiedene Eingaben, aber die zwei häufigsten Aufrufe sind unten aufgeführt:

- Wenn Sie PFX-Dateien für Ihre Signatur- und Verschlüsselungszertifikate verwenden, führen Sie die folgenden Befehle aus:

```
$signingCertPass = Read-Host -AsSecureString -Prompt "Signing certificate password"
$encryptionCertPass = Read-Host -AsSecureString -Prompt "Encryption certificate password"

Initialize-HgsServer -HgsServiceName 'MyHgsDNN' -SigningCertificatePath '.\signCert.pfx' -
SigningCertificatePassword $signingCertPass -EncryptionCertificatePath '.\encCert.pfx' -
EncryptionCertificatePassword $encryptionCertPass -TrustHostkey
```

- Wenn Sie nicht exportierbare Zertifikate verwenden, die im lokalen Zertifikat Speicher installiert sind, führen Sie den folgenden Befehl aus. Wenn Sie die Fingerabdrücke ihrer Zertifikate nicht kennen, können Sie die verfügbaren Zertifikate auflisten, indem Sie

```
Get-ChildItem Cert:\LocalMachine\My
```

 ausführen.

```
Initialize-HgsServer -HgsServiceName 'MyHgsDNN' -SigningCertificateThumbprint '1A2B3C4D5E6F...' -
EncryptionCertificateThumbprint '0F9E8D7C6B5A...' --TrustHostKey
```

4. Wenn Sie Zertifikate für Host-Überwachungsdienst Fingerabdrücke verwenden bereitgestellt, werden Sie aufgefordert, Host-Überwachungsdienst Zugriff auf den privaten Schlüssel dieser Zertifikate gewährt werden. Führen Sie auf einem Server mit Desktopdarstellung, die installiert werden soll die folgenden Schritte aus:

- a. Öffnen Sie den Zertifikat-Manager für lokalen Computer ("certlm.msc")
- b. Suchen Sie die Zertifikate > mit der rechten Maustaste > alle Aufgaben > Privatschlüssel verwalten
- c. Klicken Sie auf **Hinzufügen**.
- d. Klicken Sie im Auswahlfenster Objekt auf **Objekttypen** , und aktivieren Sie **-Dienstkonten**
- e. Geben Sie den Namen des Dienstkontos erwähnt in den Text der Warnung aus `Initialize-HgsServer`
- f. Stellen Sie sicher, dass das gruppenverwaltete Dienstkonto "Lesen" für den privaten Schlüssel zugreifen.

Auf Server Core aufweist müssen Sie ein PowerShell-Modul zur Unterstützung bei der Festlegung der Berechtigungen für den privaten Schlüssel herunterladen.

- a. Führen Sie `Install-Module GuardedFabricTools` auf dem Server-Host-Überwachungsdienst, verfügt er über Internetkonnektivität, oder führen Sie `Save-Module GuardedFabricTools` auf einem anderen Computer und kopieren Sie das Modul über den HGS-Server.
- b. Führen Sie `Import-Module GuardedFabricTools` aus. Dadurch wird zusätzliche Eigenschaften finden Sie in PowerShell zertifikatobjekten hinzugefügt.
- c. Suchen Sie den Zertifikatfingerabdruck in PowerShell mit `Get-ChildItem Cert:\LocalMachine\My`
- d. Aktualisieren Sie die ACL, und Ersetzen Sie dabei den Fingerabdruck durch Ihre eigenen und das gMSA-Konto mit dem Konto in den folgenden Code im Warnungstext aufgeführt

`Initialize-HgsServer` .

```
$certificate = Get-Item "Cert:\LocalMachine\1A2B3C..."
$certificate.Acl = $certificate.Acl | Add-AccessRule "HgsSvc_1A2B3C" Read Allow
```

Wenn Sie HSM-gesicherten Zertifikate verwenden, oder die Zertifikate, in gespeichert von Drittanbietern Key Storage Provider, diese Schritte gelten möglicherweise nicht für Sie. Dokumentation des Schlüsselspeicheranbieters für die Informationen zum Verwalten von Berechtigungen für Ihren privaten Schlüssel. In einigen Fällen steht keine Autorisierung oder Autorisierung wird für den gesamten Computer bereitgestellt, wenn das Zertifikat installiert ist.

5. Das ist alles! In einer Produktionsumgebung sollten Sie weiterhin [zusätzliche HGS-Knoten zu Ihrem Cluster hinzufügen](#).

Nächster Schritt

[Host Schlüssel erstellen](#)

Initialisieren des HGS-Clusters mithilfe des Schlüssel Modus in einer vorhandenen geschützten Gesamtstruktur

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019

« INSTALLIEREN VON HGS IN EINER
NEUEN

Gesamtstruktur

ERSTELLEN EINES HOST
SCHLÜSSELS»

Active Directory Domain Services wird auf dem Computer installiert, sollte jedoch nicht konfiguriert bleiben.

Suchen Sie Ihr HGS-Überwachungsdienst-Zertifikate. Sie benötigen ein Signaturzertifikat und ein Verschlüsselungszertifikat clientkonfigurationsobjekt des Host-Überwachungsdienst-Clusters. Die einfachste Möglichkeit zum Angeben der Zertifikate auf dem Host-Überwachungsdienst ist eine kennwortgeschützte PFX-Datei für jedes Zertifikat zu erstellen, die die öffentlichen und privaten Schlüssel enthält. Wenn Sie HSM-gesicherten Schlüsseln oder andere nicht exportierbare Zertifikate verwenden, stellen Sie sicher, dass das Zertifikat in den Zertifikatspeicher des lokalen Computers installiert ist, bevor Sie fortfahren. Weitere Informationen, welche Zertifikate verwenden können, finden Sie unter [Abrufen von Zertifikaten für die Host-Überwachungsdienst](#).

Bevor Sie fortfahren, stellen Sie sicher, dass Sie die Cluster Objekte für den Host-Überwachungsdienst vorab bereitgestellt haben, und gewähren Sie dem angemeldeten Benutzer die **vollständige Kontrolle** über die VCO- und CNO-Objekte in Active Directory. Der Name des virtuellen Computer Objekts muss an den `-HgsServiceName` -Parameter übergeben werden, und der Cluster Name muss an den `-ClusterName` -Parameter übergeben werden.

TIP

Überprüfen Sie die AD-Domänen Controller, um sicherzustellen, dass Ihre Cluster Objekte auf alle DCS repliziert wurden

Wenn Sie PFX-basierte Zertifikate verwenden, führen Sie auf dem HGS-Server die folgenden Befehle aus:

```
$signingCertPass = Read-Host -AsSecureString -Prompt "Signing certificate password"
$encryptionCertPass = Read-Host -AsSecureString -Prompt "Encryption certificate password"

Install-ADServiceAccount -Identity 'HGSgMSA'

Initialize-HgsServer -UseExistingDomain -ServiceAccount 'HGSgMSA' -JeaReviewersGroup 'HgsJeaReviewers' -
JeaAdministratorsGroup 'HgsJeaAdmins' -HgsServiceName 'HgsService' -ClusterName 'HgsCluster' -
SigningCertificatePath '.\signCert.pfx' -SigningCertificatePassword $signPass -EncryptionCertificatePath
'.\encCert.pfx' -EncryptionCertificatePassword $encryptionCertPass -TrustHostKey
```

Wenn Sie Zertifikate verwenden, die auf dem lokalen Computer installiert sind (z. B. HSM-gestützte Zertifikate und nicht exportierbare Zertifikate), verwenden Sie stattdessen die Parameter "`-SigningCertificateThumbprint`" und "`-EncryptionCertificateThumbprint`".

Initialisieren von HGS mithilfe des vom Administrator vertrauenswürdigen Nachweis

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

IMPORTANT

Der admin-Truste Nachweis (AD-Modus) ist ab Windows Server 2019 veraltet. Für Umgebungen, in denen ein TPM-Nachweis nicht möglich ist, konfigurieren Sie den [Host Schlüssel](#) Nachweis. Der Host Schlüssel Nachweis bietet eine ähnliche Garantie für den AD-Modus und ist einfacher einzurichten.

Diese Schritte sind abhängig davon, ob Sie HGS in einer neuen Gesamtstruktur oder in einer vorhandenen geschützten Gesamtstruktur initialisieren:

1. [Initialisieren des HGS-Clusters in einer neuen Gesamtstruktur \(Standard\)](#)

– Oder –

[Initialisieren des HGS-Clusters in einer vorhandenen geschützten Gesamtstruktur](#)

2. [Konfigurieren der DNS-Weiterleitung in der Fabric-Domäne](#)

3. [Konfigurieren der DNS-Weiterleitung und einer unidirektionalen Vertrauensstellung in der HGS-Domäne](#)

Initialisieren des HGS-Clusters mit dem AD-Modus in einer neuen dedizierten Gesamtstruktur (Standard)

09.04.2020 • 5 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

IMPORTANT

Der admin-Trustee Nachweis (AD-Modus) ist ab Windows Server 2019 veraltet. Für Umgebungen, in denen ein TPM-Nachweis nicht möglich ist, konfigurieren Sie den [Host Schlüssel](#) Nachweis. Der Host Schlüssel Nachweis bietet eine ähnliche Garantie für den AD-Modus und ist einfacher einzurichten.

1. Clients können einen beliebigen Knoten des Host-Überwachungsdienst mit Failover-Clusterunterstützung verteilten Netzwerknamen (DNN) problemlos kontaktieren. Sie müssen ein DNN auswählen. Dieser Name wird in den HGS DNS-Dienst registriert werden. Beispielsweise können bei 3 HGS-Knoten mit Hostnamen HGS01 HGS02 und HGS03, möglicherweise möchten Sie "Host-Überwachungsdienst" oder "HgsCluster" für das DNN auswählen.
2. Suchen Sie Ihr HGS-Überwachungsdienst-Zertifikate. Sie benötigen ein Signaturzertifikat und ein Verschlüsselungszertifikat clientkonfigurationsobjekt des Host-Überwachungsdienst-Clusters. Die einfachste Möglichkeit zum Angeben der Zertifikate auf dem Host-Überwachungsdienst ist eine kennwortgeschützte PFX-Datei für jedes Zertifikat zu erstellen, die die öffentlichen und privaten Schlüssel enthält. Wenn Sie HSM-gesicherten Schlüsseln oder andere nicht exportierbare Zertifikate verwenden, stellen Sie sicher, dass das Zertifikat in den Zertifikatspeicher des lokalen Computers installiert ist, bevor Sie fortfahren. Weitere Informationen, welche Zertifikate verwenden können, finden Sie unter [Abrufen von Zertifikaten für die Host-Überwachungsdienst](#).
3. Führen Sie [Initialize-hgsserver](#) in einem PowerShell-Fenster mit erhöhten Rechten auf dem ersten HGS-Knoten aus. Die Syntax dieses Cmdlets unterstützt viele verschiedene Eingaben, aber die zwei häufigsten Aufrufe sind unten aufgeführt:
 - Wenn Sie PFX-Dateien für Ihre Signatur- und Verschlüsselung Zertifikate verwenden, führen Sie die folgenden Befehle aus:

```
$signingCertPass = Read-Host -AsSecureString -Prompt "Signing certificate password"
$encryptionCertPass = Read-Host -AsSecureString -Prompt "Encryption certificate password"

Initialize-HgsServer -HgsServiceName 'MyHgsDNN' -SigningCertificatePath '.\signCert.pfx' -
SigningCertificatePassword $signingCertPass -EncryptionCertificatePath '.\encCert.pfx' -
EncryptionCertificatePassword $encryptionCertPass -TrustActiveDirectory
```

- Wenn Sie nicht exportierbare Zertifikate verwenden, die im lokalen Zertifikat Speicher installiert sind, führen Sie den folgenden Befehl aus. Wenn Sie die Fingerabdrücke ihrer Zertifikate nicht kennen, können Sie die verfügbaren Zertifikate auflisten, indem Sie `Get-ChildItem Cert:\LocalMachine\My` ausführen.

```
Initialize-HgsServer -HgsServiceName 'MyHgsDNN' -SigningCertificateThumbprint '1A2B3C4D5E6F...' -
EncryptionCertificateThumbprint '0F9E8D7C6B5A...' --TrustActiveDirectory
```

4. Wenn Sie Zertifikate für Host-Überwachungsdienst Fingerabdrücke verwenden bereitgestellt, werden Sie aufgefordert, Host-Überwachungsdienst Zugriff auf den privaten Schlüssel dieser Zertifikate gewährt werden. Führen Sie auf einem Server mit Desktopdarstellung, die installiert werden soll die folgenden Schritte aus:

- a. Öffnen Sie den Zertifikat-Manager für lokalen Computer ("certlm.msc")
- b. Suchen Sie die Zertifikate > mit der rechten Maustaste > alle Aufgaben > Privatschlüssel verwalten
- c. Klicken Sie auf **Hinzufügen**.
- d. Klicken Sie im Auswahlfenster Objekt auf **Objekttypen**, und aktivieren Sie **-Dienstkonten**
- e. Geben Sie den Namen des Dienstkontos erwähnt in den Text der Warnung aus `Initialize-HgsServer`
- f. Stellen Sie sicher, dass das gruppenverwaltete Dienstkonto "Lesen" für den privaten Schlüssel zugreifen.

Auf Server Core aufweist müssen Sie ein PowerShell-Modul zur Unterstützung bei der Festlegung der Berechtigungen für den privaten Schlüssel herunterladen.

- a. Führen Sie `Install-Module GuardedFabricTools` auf dem Server-Host-Überwachungsdienst, verfügt er über Internetkonnektivität, oder führen Sie `Save-Module GuardedFabricTools` auf einem anderen Computer und kopieren Sie das Modul über den HGS-Server.
- b. Führen Sie `Import-Module GuardedFabricTools` aus. Dadurch wird zusätzliche Eigenschaften finden Sie in PowerShell zertifikatobjekten hinzugefügt.
- c. Suchen Sie den Zertifikatfingerabdruck in PowerShell mit `Get-ChildItem Cert:\LocalMachine\My`
- d. Aktualisieren Sie die ACL, und Ersetzen Sie dabei den Fingerabdruck durch Ihre eigenen und das gMSA-Konto mit dem Konto in den folgenden Code im Warnungstext aufgeführt

`Initialize-HgsServer` .

```
$certificate = Get-Item "Cert:\LocalMachine\1A2B3C..."
$certificate.Acl = $certificate.Acl | Add-AccessRule "HgsSvc_1A2B3C" Read Allow
```

Wenn Sie HSM-gesicherten Zertifikate verwenden, oder die Zertifikate, in gespeichert von Drittanbietern Key Storage Provider, diese Schritte gelten möglicherweise nicht für Sie. Dokumentation des Schlüsselspeicheranbieters für die Informationen zum Verwalten von Berechtigungen für Ihren privaten Schlüssel. In einigen Fällen steht keine Autorisierung oder Autorisierung wird für den gesamten Computer bereitgestellt, wenn das Zertifikat installiert ist.

5. Das ist alles! In einer Produktionsumgebung sollten Sie weiterhin [zusätzliche HGS-Knoten zu Ihrem Cluster hinzufügen](#).

Nächster Schritt

[Konfigurieren des Fabric-DNS](#)

Initialisieren des HGS-Clusters mit dem AD-Modus in einer vorhandenen geschützten Gesamtstruktur

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

IMPORTANT

Der admin-Trustee Nachweis (AD-Modus) ist ab Windows Server 2019 veraltet. Für Umgebungen, in denen ein TPM-Nachweis nicht möglich ist, konfigurieren Sie den [Host Schlüssel](#) Nachweis. Der Host Schlüssel Nachweis bietet eine ähnliche Garantie für den AD-Modus und ist einfacher einzurichten.

Active Directory Domain Services wird auf dem Computer installiert, sollte jedoch nicht konfiguriert bleiben.

Suchen Sie Ihr HGS-Überwachungsdienst-Zertifikate. Sie benötigen ein Signaturzertifikat und ein Verschlüsselungszertifikat clientkonfigurationsobjekt des Host-Überwachungsdienst-Clusters. Die einfachste Möglichkeit zum Angeben der Zertifikate auf dem Host-Überwachungsdienst ist eine kennwortgeschützte PFX-Datei für jedes Zertifikat zu erstellen, die die öffentlichen und privaten Schlüssel enthält. Wenn Sie HSM-gesicherten Schlüsseln oder andere nicht exportierbare Zertifikate verwenden, stellen Sie sicher, dass das Zertifikat in den Zertifikatspeicher des lokalen Computers installiert ist, bevor Sie fortfahren. Weitere Informationen, welche Zertifikate verwenden können, finden Sie unter [Abrufen von Zertifikaten für die Host-Überwachungsdienst](#).

Bevor Sie fortfahren, stellen Sie sicher, dass Sie die Cluster Objekte für den Host-Überwachungsdienst vorab bereitgestellt haben, und gewähren Sie dem angemeldeten Benutzer die **vollständige Kontrolle** über die VCO- und CNO-Objekte in Active Directory. Der Name des virtuellen Computer Objekts muss an den `-HgsServiceName` -Parameter übergeben werden, und der Cluster Name muss an den `-ClusterName` -Parameter übergeben werden.

TIP

Überprüfen Sie die AD-Domänen Controller, um sicherzustellen, dass Ihre Cluster Objekte auf alle DCS repliziert wurden

Wenn Sie PFX-basierte Zertifikate verwenden, führen Sie auf dem HGS-Server die folgenden Befehle aus:

```
$signingCertPass = Read-Host -AsSecureString -Prompt "Signing certificate password"
$encryptionCertPass = Read-Host -AsSecureString -Prompt "Encryption certificate password"

Install-ADServiceAccount -Identity 'HGSgMSA'

Initialize-HgsServer -UseExistingDomain -ServiceAccount 'HGSgMSA' -JeaReviewersGroup 'HgsJeaReviewers' -
JeaAdministratorsGroup 'HgsJeaAdmins' -HgsServiceName 'HgsService' -ClusterName 'HgsCluster' -
SigningCertificatePath '.\signCert.pfx' -SigningCertificatePassword $signPass -EncryptionCertificatePath
'.\encCert.pfx' -EncryptionCertificatePassword $encryptionCertPass -TrustActiveDirectory
```

Wenn Sie Zertifikate verwenden, die auf dem lokalen Computer installiert sind (z. b. HSM-gestützte Zertifikate und nicht exportierbare Zertifikate), verwenden Sie stattdessen die Parameter "`-SigningCertificateThumbprint`" und "`-EncryptionCertificateThumbprint`".

Nächster Schritt

Konfigurieren des Fabric-DNS für geschützte Hosts

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

IMPORTANT

Der AD-Modus ist ab Windows Server 2019 veraltet. Für Umgebungen, in denen ein TPM-Nachweis nicht möglich ist, konfigurieren Sie den [Host Schlüssel](#) Nachweis. Der Host Schlüssel Nachweis bietet eine ähnliche Garantie für den AD-Modus und ist einfacher einzurichten.

Ein fabricadministrator muss das Fabric-DNS benötigt, damit überwachte Hosts den HGS-Cluster auflösen können. Der HGS-Cluster muss bereits [vom HGS-Administrator eingerichtet](#) sein.

Es gibt viele Möglichkeiten zum Konfigurieren der Namensauflösung für die Fabric-Domäne. Eine einfache Möglichkeit besteht darin, eine bedingte Weiterleitung-Zone im DNS für das Fabric zu einzurichten. Führen Sie die folgenden Befehle zum Einrichten dieser Zone in einer Windows PowerShell-Konsole mit erhöhten Rechten auf einem Fabric-DNS-Server. Ersetzen Sie den Namen und Adressen in der Windows PowerShell-Syntax finden Sie unten nach Bedarf für Ihre Umgebung. Fügen Sie der Masterserver für die zusätzlichen HGS-Knoten hinzu.

```
Add-DnsServerConditionalForwarderZone -Name 'bastion.local' -ReplicationScope "Forest" -MasterServers <IP addresses of HGS server>
```

Nächster Schritt

[Konfigurieren von HGS DNS und einer unidirektionalen Vertrauensstellung](#)

Konfigurieren der DNS-Weiterleitung in der HGS-Domäne und einer unidirektionalen Vertrauensstellung mit der Fabric-Domäne

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

IMPORTANT

Der AD-Modus ist ab Windows Server 2019 veraltet. Für Umgebungen, in denen ein TPM-Nachweis nicht möglich ist, konfigurieren Sie den [Host Schlüssel](#)Nachweis. Der Host Schlüssel Nachweis bietet eine ähnliche Garantie für den AD-Modus und ist einfacher einzurichten.

Führen Sie die folgenden Schritte aus, um die DNS-Weiterleitung einzurichten und eine unidirektionale Vertrauensstellung mit der Fabric-Domäne einzurichten. Diese Schritte ermöglichen es dem HGS, die Fabric-Domänen Controller zu finden und die Gruppenmitgliedschaft der Hyper-V-Hosts zu überprüfen.

1. Führen Sie den folgenden Befehl in einer PowerShell-Sitzung mit erhöhten Rechten aus, um die DNS-Weiterleitung Ersetzen Sie fabrikam.com durch den Namen der Fabric-Domäne, und geben Sie die IP-Adressen der DNS-Server in der Fabric-Domäne ein. Zeigen Sie auf mehr als einen DNS-Server, um eine höhere Verfügbarkeit zu erhalten.

```
Add-DnsServerConditionalForwarderZone -Name "fabrikam.com" -ReplicationScope "Forest" -MasterServers <DNSserverAddress1>, <DNSserverAddress2>
```

2. Führen Sie den folgenden Befehl an einer Eingabeaufforderung mit erhöhten Rechten aus, um eine unidirektionale Vertrauensstellung zu erstellen:

Ersetzen Sie `bastion.local` durch den Namen der HGS-Domäne, und `fabrikam.com` Sie durch den Namen der Fabric-Domäne. Geben Sie das Kennwort für einen Administrator der Fabric-Domäne an.

```
netdom trust bastion.local /domain:fabrikam.com /userD:fabrikam.com\Administrator /passwordD:<password> /add
```

Nächster Schritt

[Konfigurieren von HTTPS](#)

Konfigurieren von HGS für die HTTPS-Kommunikation

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Wenn Sie den HGS-Server initialisieren, werden die IIS-Websites standardmäßig für die HTTP-Kommunikation konfiguriert. Alle sensiblen Materialien, die an und von HGS übermittelt werden, werden immer mithilfe der Verschlüsselung auf Nachrichten Ebene verschlüsselt. Wenn Sie jedoch ein höheres Maß an Sicherheit wünschen, können Sie auch HTTPS aktivieren, indem Sie HGS mit einem SSL-Zertifikat konfigurieren.

Rufen Sie zunächst ein SSL-Zertifikat für Host-Überwachungsdienst, von Ihrer Zertifizierungsstelle. Jeden Hostcomputer muss das SSL-Zertifikat vertrauen, daher wird empfohlen, dass Sie das SSL-Zertifikat von Ihres Unternehmens public Key-Infrastruktur oder Drittanbieters Zertifizierungsstelle ausgeben. Beliebiges SSL-Zertifikat, das von IIS unterstützt wird jedoch vom Host-Überwachungsdienst bietet unterstützt **Name des Antragstellers des Zertifikats muss der vollqualifizierte Name des Host-Überwachungsdienst-Dienst entsprechen** (verteilter Netzwerkname Cluster). Beispielsweise sollte die Host-Überwachungsdienst-Domäne ist "bastion.local" und den Namen des Host-Überwachungsdienst-Diensts ist "Host-Überwachungsdienst", das SSL-Zertifikat für "hgs.bastion.local" ausgegeben werden. Sie können das Zertifikat der alternative Antragstellernamen bei Bedarf zusätzliche DNS-Namen hinzufügen.

Nachdem Sie die SSL-Zertifikat, öffnen Sie eine PowerShell-Sitzung mit erhöhten Rechten verfügen, und geben Sie entweder den Zertifikatpfad beim Ausführen von [Set-HgsServer](#):

```
$sslPassword = Read-Host -AsSecureString -Prompt "SSL Certificate Password"
Set-HgsServer -Http -Https -HttpsCertificatePath 'C:\temp\HgsSSLCertificate.pfx' -HttpsCertificatePassword $sslPassword
```

Oder, wenn Sie das Zertifikat bereits im lokalen Zertifikatspeicher installiert haben, können Sie es durch Fingerabdruck verweisen:

```
Set-HgsServer -Http -Https -HttpsCertificateThumbprint 'A1B2C3D4E5F6...'
```

IMPORTANT

Konfigurieren von Host-Überwachungsdienst mit einem SSL-Zertifikat wird den HTTP-Endpunkt nicht deaktiviert werden. Wenn Sie nur die Verwendung von HTTPS-Endpunkt zulassen möchten, konfigurieren Sie Windows-Firewall so, dass eingehende Verbindungen an Port 80 blockiert. **Ändern Sie die IIS-Bindungen nicht** für Host-Überwachungsdienst Websites So entfernen Sie den HTTP-Endpunkt an; es wird nicht unterstützt. zu diesem Zweck.

Konfigurieren zusätzlicher HGS-Knoten

09.04.2020 • 11 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

In Produktionsumgebungen sollten HGS in einem Cluster mit hoher Verfügbarkeit eingerichtet werden, um sicherzustellen, dass abgeschränkte VMS auch dann eingeschaltet werden können, wenn ein HGS-Knoten ausfällt. Für Testumgebungen sind keine sekundären HGS-Knoten erforderlich.

Verwenden Sie eine dieser Methoden, um HGS-Knoten hinzuzufügen, die für Ihre Umgebung am besten geeignet sind.

Neue HGS-Gesamtstruktur	Verwenden von PFX-Dateien	Verwenden von Zertifikat Fingerabdrücken
Vorhandene geschützte Gesamtstruktur	Verwenden von PFX-Dateien	Verwenden von Zertifikat Fingerabdrücken

Erforderliche Komponenten

Stellen Sie sicher, dass jeder zusätzliche Knoten:

- Hat dieselbe Hardware- und Softwarekonfiguration wie der primäre Knoten.
- Ist mit dem gleichen Netzwerk verbunden wie die anderen HGS-Server
- Kann die anderen HGS-Server anhand Ihrer DNS-Namen auflösen

Dedizierte HGS-Gesamtstruktur mit PFX-Zertifikaten

1. Herauf Stufen des HGS-Knotens zu einem Domänen Controller
2. Initialisieren des HGS-Servers

Herauf Stufen des HGS-Knotens zu einem Domänen Controller

1. Führen Sie [Install-HgsServer](#) zum Beitreten zur Domäne und den Knoten zu einem Domänencontroller heraufstufen.

```
$adSafeModePassword = ConvertTo-SecureString -AsPlainText '<password>' -Force  
  
$cred = Get-Credential 'relecloud\Administrator'  
  
Install-HgsServer -HgsDomainName 'bastion.local' -HgsDomainCredential $cred -  
SafeModeAdministratorPassword $adSafeModePassword -Restart
```

2. Beim Neustart des Servers, melden Sie sich mit einem Domänenadministratorkonto an.

Initialisieren des HGS-Servers

Führen Sie den folgenden Befehl auf dem vorhandenen Host-Überwachungsdienst-Cluster beitreten.

```
Initialize-HgsServer -HgsServerIPAddress <IP address of first HGS Server>
```

Dedizierte HGS-Gesamtstruktur mit Zertifikat Fingerabdrücken

1. Herauf Stufen des HGS-Knotens zu einem Domänen Controller
2. Initialisieren des HGS-Servers
3. Installieren der privaten Schlüssel für die Zertifikate

Herauf Stufen des HGS-Knotens zu einem Domänen Controller

1. Führen Sie [Install-HgsServer](#) zum Beitreten zur Domäne und den Knoten zu einem Domänencontroller heraufstufen.

```
$adSafeModePassword = ConvertTo-SecureString -AsPlainText '<password>' -Force

$cred = Get-Credential 'relecloud\Administrator'

Install-HgsServer -HgsDomainName 'bastion.local' -HgsDomainCredential $cred -
SafeModeAdministratorPassword $adSafeModePassword -Restart
```

2. Beim Neustart des Servers, melden Sie sich mit einem Domänenadministratorkonto an.

Initialisieren des HGS-Servers

Führen Sie den folgenden Befehl auf dem vorhandenen Host-Überwachungsdienst-Cluster beitreten.

```
Initialize-HgsServer -HgsServerIPAddress <IP address of first HGS Server>
```

Installieren der privaten Schlüssel für die Zertifikate

Wenn Sie eine PFX-Datei nicht für die Verschlüsselung und Signaturzertifikate auf dem ersten HGS-Server angegeben haben, wird nur der öffentliche Schlüssel mit diesem Server repliziert werden. Sie müssen den privaten Schlüssel durch Importieren einer PFX-Datei mit dem privaten Schlüssel, in den lokalen Zertifikatspeicher oder, im Fall von HSM-gesicherten Schlüsseln, installieren den Softwareschlüsselspeicher-Anbieter konfigurieren und Ihre Zertifikate pro Ihres HSM-Herstellers zuordnen Anweisungen.

Vorhandene geschützte Gesamtstruktur mit PFX-Zertifikaten

1. Fügen Sie den Knoten der vorhandenen Domäne hinzu.
2. Erteilen Sie dem Computer Rechte zum Abrufen des GMSA-Kennworts und Ausführen von Install-ADServiceAccount.
3. Initialisieren des HGS-Servers

Fügen Sie den Knoten der vorhandenen Domäne hinzu.

1. Stellen Sie sicher, dass mindestens eine NIC auf dem Knoten für die Verwendung des DNS-Servers auf dem ersten HGS-Server konfiguriert ist.
2. Verknüpfen Sie den neuen HGS-Knoten mit derselben Domäne wie der erste HGS-Knoten.

Erteilen Sie dem Computer Rechte zum Abrufen des GMSA-Kennworts und Ausführen von Install-ADServiceAccount.

1. Haben Sie eine Directory Services-Administrator das Computerkonto für unseren neuen Knoten hinzufügen, der Sicherheitsgruppe, die mit allen Ihren HGS-Servern, die Berechtigungen festgelegt haben, können von diesen Servern das gMSA-Konto-Host-Überwachungsdienst verwendet wird.
2. Starten Sie den neuen Knoten um ein neues Kerberos-Ticket zu erhalten, das der Computer die Mitgliedschaft in dieser Sicherheitsgruppe enthält neu. Wenn der Neustart abgeschlossen ist, melden Sie sich eine Domänenidentität, zu der der lokalen Administratorengruppe auf dem Computer gehört.
3. Installieren Sie den Host-Überwachungsdienst gruppenverwalteten Dienstkontos auf dem Knoten.

```
Install-ADServiceAccount -Identity <HGSgMSAAccount>
```

Initialisieren des HGS-Servers

Führen Sie den folgenden Befehl auf dem vorhandenen Host-Überwachungsdienst-Cluster beitreten.

```
Initialize-HgsServer -HgsServerIPAddress <IP address of first HGS Server>
```

Vorhandene geschützte Gesamtstruktur mit Zertifikat Fingerabdruck

1. Fügen Sie den Knoten der vorhandenen Domäne hinzu.
2. Erteilen Sie dem Computer Rechte zum Abrufen des GMSA-Kennworts und Ausführen von Install-ADServiceAccount.
3. Initialisieren des HGS-Servers
4. Installieren der privaten Schlüssel für die Zertifikate

Fügen Sie den Knoten der vorhandenen Domäne hinzu.

1. Stellen Sie sicher, dass mindestens eine NIC auf dem Knoten für die Verwendung des DNS-Servers auf dem ersten HGS-Server konfiguriert ist.
2. Verknüpfen Sie den neuen HGS-Knoten mit derselben Domäne wie der erste HGS-Knoten.

Erteilen Sie dem Computer Rechte zum Abrufen des GMSA-Kennworts und Ausführen von Install-ADServiceAccount.

1. Haben Sie eine Directory Services-Administrator das Computerkonto für unseren neuen Knoten hinzufügen, der Sicherheitsgruppe, die mit allen Ihren HGS-Servern, die Berechtigungen festgelegt haben, können von diesen Servern das gMSA-Konto-Host-Überwachungsdienst verwendet wird.
2. Starten Sie den neuen Knoten um ein neues Kerberos-Ticket zu erhalten, das der Computer die Mitgliedschaft in dieser Sicherheitsgruppe enthält neu. Wenn der Neustart abgeschlossen ist, melden Sie sich eine Domänenidentität, zu der der lokalen Administratorengruppe auf dem Computer gehört.
3. Installieren Sie den Host-Überwachungsdienst gruppenverwalteten Dienstkontos auf dem Knoten.

```
Install-ADServiceAccount -Identity <HGSgMSAAccount>
```

Initialisieren des HGS-Servers

Führen Sie den folgenden Befehl auf dem vorhandenen Host-Überwachungsdienst-Cluster beitreten.

```
Initialize-HgsServer -HgsServerIPAddress <IP address of first HGS Server>
```

Es dauert bis zu 10 Minuten, bis die Verschlüsselungs- und Signatur Zertifikate vom ersten HGS-Server auf diesen Knoten repliziert werden.

Installieren der privaten Schlüssel für die Zertifikate

Wenn Sie eine PFX-Datei nicht für die Verschlüsselung und Signaturzertifikate auf dem ersten HGS-Server angegeben haben, wird nur der öffentliche Schlüssel mit diesem Server repliziert werden. Sie müssen den privaten Schlüssel durch Importieren einer PFX-Datei mit dem privaten Schlüssel, in den lokalen Zertifikatspeicher oder, im Fall von HSM-gesicherten Schlüsseln, installieren den Softwareschlüsselspeicher-Anbieter konfigurieren und Ihre Zertifikate pro Ihres HSM-Herstellers zuordnen Anweisungen.

Konfigurieren von HGS für die HTTPS-Kommunikation

Wenn Sie HGS-Endpunkte mit einem SSL-Zertifikat sichern möchten, müssen Sie das SSL-Zertifikat auf diesem Knoten sowie alle anderen Knoten im HGS-Cluster konfigurieren. SSL-Zertifikate *werden nicht* von HGS repliziert und müssen nicht die gleichen Schlüssel für jeden Knoten verwenden (d. h., Sie können für jeden Knoten unterschiedliche SSL-Zertifikate verwenden).

Wenn Sie ein SSL-Zertifikat anfordern, stellen Sie sicher, dass der voll qualifizierte Cluster Domänen Name (wie in der Ausgabe von `Get-HgsServer`) entweder der allgemeine Antragsteller Name des Zertifikats ist oder als alternativer Antragsteller Name angegeben ist. Wenn Sie ein Zertifikat von Ihrer Zertifizierungsstelle erhalten haben, können Sie HGS so konfigurieren, dass es mit [Set-hgsserver](#) verwendet wird.

```
$sslPassword = Read-Host -AsSecureString -Prompt "SSL Certificate Password"
Set-HgsServer -Http -Https -HttpsCertificatePath 'C:\temp\HgsSSLCertificate.pfx' -HttpsCertificatePassword $sslPassword
```

Wenn Sie das Zertifikat bereits im lokalen Zertifikat Speicher installiert haben und es per Fingerabdruck referenzieren möchten, führen Sie stattdessen den folgenden Befehl aus:

```
Set-HgsServer -Http -Https -HttpsCertificateThumbprint 'A1B2C3D4E5F6...'
```

HGS macht immer die HTTP- und HTTPS-Ports für die Kommunikation verfügbar. Das Entfernen der HTTP-Bindung in IIS wird nicht unterstützt. Sie können jedoch die Windows-Firewall oder andere netzwerkfirewalltechnologien verwenden, um die Kommunikation über Port 80 zu blockieren.

Außerbetriebsetzen eines HGS-Knotens

So setzen Sie einen HGS-Knoten außer Betrieb:

1. [Löschen Sie die HGS-Konfiguration](#).

Dadurch wird der Knoten aus dem Cluster entfernt und der Nachweis und die Schlüsselschutz Dienste deinstalliert. Wenn es sich um den letzten Knoten im Cluster handelt, wird-Force benötigt, um anzugeben, dass der letzte Knoten entfernt und der Cluster in Active Directory zerstört werden soll.

Wenn HGS in einer geschützten Gesamtstruktur (Standard) bereitgestellt wird, ist dies der einzige Schritt. Optional können Sie den Computer aus der Domäne entfernen und das GMSA-Konto aus Active Directory entfernen.

2. Wenn HGS eine eigene Domäne erstellt haben, sollten Sie auch [HGS deinstallieren](#), um den Beitritt zur Domäne zu entfernen und den Domänen Controller herabzusetzen.

Bereitstellen geschützter Hosts

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

In den Themen in diesem Abschnitt werden die Schritte beschrieben, die ein Fabric-Administrator zum Konfigurieren von Hyper-V-Hosts für die Verwendung mit dem Host-Überwachungsdienst (HGS) durchführt. Bevor Sie diese Schritte ausführen können, muss mindestens ein Knoten im [HGS-Cluster eingerichtet werden](#).

Für TPM-Trusted Nachweis:

1. [Konfigurieren des Fabric-DNS](#): erläutert, wie Sie eine DNS-Weiterleitung von der Fabric-Domäne zur HGS-Domäne einrichten.
2. [Von HGS benötigte Erfassungsinformationen](#): erläutert, wie TPM-IDs (auch als Plattform-Bezeichner bezeichnet) erfasst, eine Code-Integritätsrichtlinie erstellt und eine TPM-Baseline erstellt wird. Anschließend geben Sie diese Informationen für den HGS-Administrator an, um den Nachweis zu konfigurieren.
3. [Bestätigen, dass geschützte Hosts bestätigen können](#)

Für Host-Schlüssel-Nachweis:

1. [Erstellen eines Host-Schlüssels](#): erläutert, wie Sie eine DNS-Weiterleitung von der Fabric-Domäne zur HGS-Domäne einrichten.
2. [Hinzufügen des Host-Schlüssels zum Nachweis-Dienst](#): erläutert das Einrichten einer Active Directory-Sicherheitsgruppe in der Fabric-Domäne, das Hinzufügen von überwachten Hosts als Mitglieder dieser Gruppe und das Bereitstellen dieser Gruppen-ID für den HGS-Administrator.
3. [Bestätigen, dass geschützte Hosts bestätigen können](#)

Für admin-Trusted Nachweis:

1. [Konfigurieren des Fabric-DNS](#): erläutert, wie Sie eine DNS-Weiterleitung von der Fabric-Domäne zur HGS-Domäne einrichten.
2. [Erstellen einer Sicherheitsgruppe](#): erläutert, wie Sie eine Active Directory-Sicherheitsgruppe in der Fabric-Domäne einrichten, überwachte Hosts als Mitglieder dieser Gruppe hinzufügen und diese Gruppen-ID dem HGS-Administrator bereitstellen.
3. [Bestätigen, dass geschützte Hosts bestätigen können](#)

Siehe auch

- [Bereitstellungsaufgaben für geschützte Fabrics und abgeschirmte VMS](#)

Voraussetzungen für geschützte Hosts

09.04.2020 • 5 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Überprüfen Sie die Host Voraussetzungen für den Nachweis Modus, den Sie ausgewählt haben, und klicken Sie dann auf den nächsten Schritt, um geschützte Hosts hinzuzufügen.

TPM-vertrauenswürdiger Nachweis

Geschützte Hosts, die den TPM-Modus verwenden, müssen die folgenden Voraussetzungen erfüllen:

- **Hardware:** für die erste Bereitstellung ist ein Host erforderlich. Zum Testen der Hyper-V-Live Migration für abgeschirmte VMS müssen Sie über mindestens zwei Hosts verfügen.

Hosts müssen über Folgendes verfügen:

- IOMMU und Second Level Address Translation (slat)
 - TPM 2.0
 - UEFI 2.3.1 oder höher
 - Konfiguriert für den Start mit UEFI (nicht im BIOS-oder Legacy Modus)
 - Sicherer Start aktiviert
- **Betriebssystem:** Windows Server 2016 Datacenter Edition oder höher

IMPORTANT

Stellen Sie sicher, dass Sie das [neueste kumulative Update](#) installieren.

- **Rolle und Features:** Hyper-v-Rolle und die Hyper-v-Unterstützung des Host-Überwachungs Diensts. Die Hyper-V-Unterstützung des Host-Überwachungs Diensts ist nur in den Datacenter-Editionen von Windows Server verfügbar.

WARNING

Die Hyper-V-Unterstützung des Host-Überwachungs Diensts ermöglicht den virtualisierungsbasierten Schutz der Code Integrität, der möglicherweise mit einigen Geräten nicht kompatibel ist. Wir empfehlen dringend, diese Konfiguration in Ihrem Lab zu testen, bevor Sie diese Funktion aktivieren. Andernfalls kann es zu unerwarteten Fehlern und sogar zu Datenverlusten oder zu einem Bluescreen (STOP-Fehler) kommen. Weitere Informationen finden Sie unter [kompatible Hardware mit Windows Server-virtualisierungsbasierter Schutz der Code Integrität](#).

Nächster Schritt:

[TPM-Informationen erfassen](#)

Host Schlüssel Nachweis

Geschützte Hosts, die den Host Schlüssel Nachweis verwenden, müssen die folgenden Voraussetzungen erfüllen:

- **Hardware:** jeder Server, der Hyper-V ab Windows Server 2019 ausführen können soll
- **Betriebssystem:** Windows Server 2019 Datacenter Edition

- **Rolle und Features:** Hyper-v-Rolle und die Hyper-v-Unterstützung des Host-Überwachungs Diensts

Der Host kann entweder einer Domäne oder einer Arbeitsgruppe hinzugefügt werden.

Bei einem Host Schlüssel Nachweis muss auf HGS Windows Server 2019 ausgeführt werden, und es muss ein v2-Nachweis ausgeführt werden. Weitere Informationen finden Sie unter [Voraussetzungen für HGS](#).

Nächster Schritt:

[Erstellen eines Schlüssel Paares](#)

Admin-vertrauenswürdiger Nachweis

IMPORTANT

Der admin-Trusted Nachweis (AD-Modus) ist ab Windows Server 2019 veraltet. Für Umgebungen, in denen ein TPM-Nachweis nicht möglich ist, konfigurieren Sie den [Host Schlüssel](#)Nachweis. Der Host Schlüssel Nachweis bietet eine ähnliche Garantie für den AD-Modus und ist einfacher einzurichten.

Hyper-V-Hosts müssen die folgenden Voraussetzungen für den AD-Modus erfüllen:

- **Hardware:** alle Server, die Hyper-V ausführen können, beginnen mit Windows Server 2016. Ein Host ist für die erste Bereitstellung erforderlich. Um die Hyper-V-Live Migration für abgeschirmte VMS zu testen, benötigen Sie mindestens zwei Hosts.
- **Betriebssystem:** Windows Server 2016 Datacenter Edition

IMPORTANT

Installieren Sie das [neueste kumulative Update](#).

- **Rolle und Features:** Hyper-v-Rolle und die Hyper-v-Unterstützung des Host-Überwachungs Features, die nur in Windows Server 2016 Datacenter Edition verfügbar ist.

WARNING

Die Hyper-V-Unterstützung des Host-Überwachungs Diensts ermöglicht den virtualisierungsbasierten Schutz der Code Integrität, der möglicherweise mit einigen Geräten nicht kompatibel ist. Wir empfehlen dringend, diese Konfiguration in Ihrem Lab zu testen, bevor Sie diese Funktion aktivieren. Andernfalls kann es zu unerwarteten Fehlern und sogar zu Datenverlusten oder zu einem Bluescreen (STOP-Fehler) kommen. Weitere Informationen finden Sie unter [kompatible Hardware mit Windows Server 2016 Virtualization-basierter Schutz der Code Integrität](#).

Nächster Schritt:

[Geschützte Hosts in einer Sicherheitsgruppe platzieren](#)

Autorisieren von überwachten Hosts mithilfe von TPM-basiertem Nachweis

09.04.2020 • 17 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Der TPM-Modus verwendet einen TPM-Bezeichner (auch als Platt Form Bezeichner oder Endorsement Key [ekpub] bezeichnet), um zu bestimmen, ob ein bestimmter Host als "geschützt" autorisiert ist. Bei diesem Nachweis werden sichere Start- und Code Integritäts Messungen verwendet, um sicherzustellen, dass sich ein bestimmter Hyper-V-Host in einem fehlerfreien Zustand befindet und nur vertrauenswürdiger Code ausgeführt wird. Damit der Nachweis weiß, was nicht fehlerfrei ist, müssen Sie die folgenden Artefakte erfassen:

1. TPM-Bezeichner (ekpub)
 - Diese Informationen sind für jeden Hyper-V-Host eindeutig.
2. TPM-Baseline (Start Messungen)
 - Dies gilt für alle Hyper-V-Hosts, die auf derselben Hardware Klasse ausgeführt werden.
3. Code Integritätsrichtlinie (eine Whitelist zulässiger Binärdateien)
 - Dies gilt für alle Hyper-V-Hosts, die gemeinsame Hardware und Software gemeinsam verwenden.

Es wird empfohlen, die Baseline- und CI-Richtlinie von einem "Verweis Host" zu erfassen, der für jede eindeutige Klasse der Hyper-V-Hardwarekonfiguration innerhalb Ihres Rechenzentrums repräsentativ ist. Ab Windows Server, Version 1709, sind die CI-Beispiel Richtlinien unter `c:\windows\schemas\codeintegrity\examplepolicies` enthalten.

Nachweis Richtlinien mit Versions Angabe

In Windows Server 2019 wird eine neue Methode für den Nachweis namens " v2-Nachweis" eingeführt, in der ein TPM-Zertifikat vorhanden sein muss, um die ekpub-Datei zu HGS hinzuzufügen. Mit der in Windows Server 2016 verwendeten v1-Nachweismethode konnten Sie diese Sicherheitsüberprüfung außer Kraft setzen, indem Sie das Flag "-Force" angeben, wenn Sie "Add-hgsattestationtpmhost" oder andere TPM-Nachweis-Cmdlets ausführen, um die Artefakte zu erfassen. Ab Windows Server 2019 wird der V2-Nachweis standardmäßig verwendet, und Sie müssen das Flag "-PolicyVersion v1" angeben, wenn Sie "Add-hgsattestationtpmhost" ausführen müssen, wenn Sie ein TPM ohne Zertifikat registrieren müssen. Das Flag-Force funktioniert nicht mit dem V2-Nachweis.

Ein Host kann nur überzeugen, ob für alle Artefakte (ekpub + TPM-Baseline und CI-Richtlinie) dieselbe Version des Nachweis verwendet wird. Der V2-Nachweis wird zuerst ausprobiert, und wenn dies nicht möglich ist, wird der v1-Nachweis verwendet. Dies bedeutet Folgendes: Wenn Sie eine TPM-ID mithilfe des v1-Nachweis registrieren müssen, müssen Sie auch das Flag "-PolicyVersion v1" angeben, um den v1-Nachweis zu verwenden, wenn Sie die TPM-Baseline erfassen und die CI-Richtlinie erstellen. Wenn die TPM-Baseline und die CI-Richtlinie mit dem V2-Nachweis erstellt wurden und Sie später einen überwachten Host ohne TPM-Zertifikat hinzufügen müssen, müssen Sie jedes artefaktelement mit dem Flag "-PolicyVersion v1" neu erstellen.

Erfassen Sie den TPM-Bezeichner (Platt Form Bezeichner oder ekpub) für jeden Host.

1. Stellen Sie in der Fabric-Domäne sicher, dass das TPM auf den einzelnen Hosts zur Verwendung bereit ist, d. h., das TPM ist initialisiert, und der Besitz wurde abgerufen. Sie können den Status des TPM überprüfen, indem Sie die TPM-Verwaltungskonsolle (TPM. msc) öffnen oder **Get-TPM** in einem Windows PowerShell-

Fenster mit erhöhten Rechten ausführen. Wenn das TPM nicht den Status **bereit** aufweist, müssen Sie es initialisieren und dessen Besitz festlegen. Dies kann in der TPM-Verwaltungskonsole oder durch Ausführen von **Initialize-TPM** erfolgen.

2. Führen Sie auf jedem überwachten Host den folgenden Befehl in einer Windows PowerShell-Konsole mit erhöhten Rechten aus, um die ekpub-Datei abzurufen. Ersetzen Sie für `<HostName>` den eindeutigen Hostnamen durch etwas, das zum Identifizieren dieses Hosts geeignet ist. Dabei kann es sich um den Hostnamen oder den Namen handeln, der von einem Fabric-Inventur Dienst (falls verfügbar) verwendet wird. Benennen Sie die Ausgabedatei unter Verwendung des Hostnamens.

```
(Get-PlatformIdentifier -Name '<HostName>').InnerXml | Out-file <Path><HostName>.xml -Encoding UTF8
```

3. Wiederholen Sie die vorherigen Schritte für jeden Host, der zu einem überwachten Host werden soll, und stellen Sie sicher, dass jede XML-Datei einen eindeutigen Namen erhält
4. Stellen Sie die resultierenden XML-Dateien für den HGS-Administrator bereit.
5. Öffnen Sie in der HGS-Domäne eine Windows PowerShell-Konsole mit erhöhten Rechten auf einem HGS-Server, und führen Sie den folgenden Befehl aus. Wiederholen Sie den Befehl für jede der XML-Dateien.

```
Add-HgsAttestationTpmHost -Path <Path><Filename>.xml -Name <HostName>
```

NOTE

Wenn beim Hinzufügen eines TPM-Bezeichners zu einem nicht vertrauenswürdigen Endorsement Key-Zertifikat (ekcert) ein Fehler auftritt, stellen Sie sicher, dass die [vertrauenswürdigen TPM](#) -Stamm Zertifikate dem HGS-Knoten hinzugefügt wurden. Darüber hinaus verwenden einige TPM-Anbieter keine ekcerts. Sie können überprüfen, ob ein ekcert fehlt, indem Sie die XML-Datei in einem Editor wie z. B. Editor öffnen und auf eine Fehlermeldung mit dem Hinweis, dass kein ekcert gefunden wurde, prüfen. Wenn dies der Fall ist und Sie sich darauf verlassen, dass das TPM auf dem Computer authentisch ist, können Sie den `-Force` -Parameter verwenden, um den Host Bezeichner zu HGS hinzuzufügen. In Windows Server 2019 müssen Sie auch den `-PolicyVersion v1` -Parameter verwenden, wenn Sie `-Force` verwenden. Dadurch wird eine Richtlinie erstellt, die mit dem Verhalten von Windows Server 2016 konsistent ist, und Sie müssen beim Registrieren der CI-Richtlinie und der TPM-Baseline auch `-PolicyVersion v1` verwenden.

Erstellen und Anwenden einer Code Integritätsrichtlinie

Mit einer Code Integritätsrichtlinie kann sichergestellt werden, dass nur die ausführbaren Dateien, denen Sie Vertrauen, auf einem Host ausgeführt werden dürfen, ausgeführt werden dürfen. Schadsoftware und andere ausführbare Dateien außerhalb der vertrauenswürdigen ausführbaren Dateien können nicht ausgeführt werden.

Für jeden überwachten Host muss eine Code Integritätsrichtlinie angewendet werden, damit abgeschirmte VMS im TPM-Modus ausgeführt werden können. Sie geben die exakten Code Integritäts Richtlinien an, denen Sie Vertrauen, indem Sie Sie zu HGS hinzufügen. Code Integritäts Richtlinien können konfiguriert werden, um die Richtlinie zu erzwingen, jegliche Software zu blockieren, die die Richtlinie nicht einhält, oder einfach ein Ereignis zu überwachen (protokollieren, wenn Software, die nicht in der Richtlinie definiert ist).

Ab Windows Server, Version 1709, sind Beispielcode Integritäts Richtlinien in Windows unter `c:\windows\schemas\codeintegrity\examplepolicies` enthalten. Für Windows Server werden zwei Richtlinien empfohlen:

- **Allowmicrosoft:** erlaubt alle Dateien, die von Microsoft signiert wurden. Diese Richtlinie wird für Server Anwendungen, z. B. SQL oder Exchange, empfohlen, oder wenn der Server von Agents überwacht wird, die von Microsoft veröffentlicht wurden.

- **DefaultWindows_Enforced:** erlaubt nur Dateien, die in Windows enthalten sind und keine anderen von Microsoft veröffentlichten Anwendungen, wie z. b. Office, zulässt. Diese Richtlinie wird für Server empfohlen, auf denen nur integrierte Server Rollen und Features wie z. b. Hyper-V ausgeführt werden.

Es wird empfohlen, zuerst die CI-Richtlinie im Überwachungsmodus (Protokollierungs Modus) zu erstellen, um festzustellen, ob Sie etwas hat, und dann die Richtlinie für Host produktionsworkloads zu erzwingen.

Wenn Sie das Cmdlet " [New-cipolicy](#) " verwenden, um eine eigene Code Integritätsrichtlinie zu generieren, müssen Sie die zu verwendenden Regel Ebenen festlegen. Wir empfehlen eine primäre Ebene des **Verlegers** mit Fall Back auf **Hash**, sodass die meisten digital signierten Software aktualisiert werden kann, ohne die CI-Richtlinie zu ändern. Neue Software, die vom selben Verleger geschrieben wird, kann auch auf dem Server installiert werden, ohne dass die CI-Richtlinie geändert wird. Ausführbare Dateien, die nicht digital signiert sind, werden Hashwerte aufweisen: bei Updates für diese Dateien müssen Sie eine neue CI-Richtlinie erstellen. Weitere Informationen zu den verfügbaren CI-Richtlinien Regel Ebenen finden Sie unter Bereitstellen von [Code Integritäts Richtlinien: Richtlinien Regeln und Datei Regeln](#) und Cmdlet-Hilfe.

1. Generieren Sie auf dem Referenz Host eine neue Code Integritätsrichtlinie. Die folgenden Befehle erstellen eine Richtlinie auf **Verleger** Ebene mit Fall Back auf **Hash**. Anschließend wird die XML-Datei in das Binärdatei Format konvertiert, und HGS müssen die CI-Richtlinie anwenden bzw. messen.

```
New-CIPolicy -Level Publisher -Fallback Hash -FilePath 'C:\temp\HW1CodeIntegrity.xml' -UserPEs  
  
ConvertFrom-CIPolicy -XmlFilePath 'C:\temp\HW1CodeIntegrity.xml' -BinaryFilePath  
'C:\temp\HW1CodeIntegrity.p7b'
```

NOTE

Der obige Befehl erstellt eine CI-Richtlinie nur im Überwachungsmodus. Nicht autorisierte Binärdateien können nicht auf dem Host ausgeführt werden. Sie sollten nur erzwungene Richtlinien in der Produktionsumgebung verwenden.

2. Behalten Sie die Datei mit der Code Integritätsrichtlinie (XML-Datei) bei, wo Sie Sie leicht finden können. Sie müssen diese Datei zu einem späteren Zeitpunkt bearbeiten, um die CI-Richtlinie zu erzwingen oder Änderungen von zukünftigen Updates, die im System vorgenommen wurden, zusammenzuführen.
3. Anwenden der CI-Richtlinie auf den Verweis Host:
 - a. Führen Sie den folgenden Befehl aus, um den Computer zur Verwendung Ihrer CI-Richtlinie zu konfigurieren. Sie können die CI-Richtlinie auch mit [Gruppenrichtlinie](#) oder [System Center Virtual Machine Manager](#) bereitstellen.

```
Invoke-CimMethod -Namespace root/Microsoft/Windows/CI -ClassName PS_UpdateAndCompareCIPolicy -  
MethodName Update -Arguments @{ FilePath = "C:\temp\HW1CodeIntegrity.p7b" }
```

- b. Starten Sie den Host neu, um die Richtlinie anzuwenden.
4. Testen Sie die Code Integritätsrichtlinie, indem Sie eine typische Arbeitsauslastung ausführen. Hierzu zählen u. a. die Ausführung von VMS, fabricverwaltungs-Agents, Sicherungs-Agents oder Tools zur Problembehandlung auf dem Computer. Überprüfen Sie, ob Code Integritäts Verletzungen vorliegen, und aktualisieren Sie ggf. die CI-Richtlinie.
 5. Ändern Sie die CI-Richtlinie in den erzwungenen Modus, indem Sie die folgenden Befehle für die aktualisierte CI-Richtlinien-XML-Datei ausführen

```
Set-RuleOption -FilePath 'C:\temp\HW1CodeIntegrity.xml' -Option 3 -Delete

ConvertFrom-CIPolicy -XmlFilePath 'C:\temp\HW1CodeIntegrity.xml' -BinaryFilePath
'C:\temp\HW1CodeIntegrity_enforced.p7b'
```

6. Wenden Sie die CI-Richtlinie auf alle Ihre Hosts (mit identischer Hardware-und Softwarekonfiguration) mithilfe der folgenden Befehle an:

```
Invoke-CimMethod -Namespace root/Microsoft/Windows/CI -ClassName PS_UpdateAndCompareCIPolicy -
MethodName Update -Arguments @{ FilePath = "C:\temp\HW1CodeIntegrity.p7b" }

Restart-Computer
```

NOTE

Seien Sie vorsichtig, wenn Sie CI-Richtlinien auf Hosts anwenden und Software auf diesen Computern aktualisieren. Alle Kernelmodustreiber, die nicht mit der CI-Richtlinie kompatibel sind, können verhindern, dass der Computer gestartet wird.

7. Stellen Sie die Binärdatei (in diesem Beispiel HW1CodeIntegrity_erzwungen. p7b) für den HGS-Administrator bereit.
8. Kopieren Sie in der HGS-Domäne die Code Integritätsrichtlinie auf einen HGS-Server, und führen Sie den folgenden Befehl aus.

Geben Sie für `<PolicyName>` einen Namen für die CI-Richtlinie ein, die den Hosttyp beschreibt, auf den Sie angewendet wird. Eine bewährte Vorgehensweise besteht darin, den Namen nach dem Make/Model Ihres Computers und allen darauf laufenden speziellen Software Konfigurationen zu benennen.

Geben Sie für `<Path>` den Pfad und den Dateinamen der Code Integritätsrichtlinie an.

```
Add-HgsAttestationCIPolicy -Path <Path> -Name '<PolicyName>'
```

Erfassen der TPM-Baseline für jede eindeutige Hardware Klasse

Eine TPM-Baseline ist für jede eindeutige Hardware Klasse in Ihrer Rechenzentrums Struktur erforderlich. Verwenden Sie erneut einen "Verweis Host".

1. Stellen Sie auf dem Referenz Host sicher, dass die Hyper-v-Rolle und die Hyper-v-Unterstützung des Host-Überwachungs Diensts installiert sind.

WARNING

Die Hyper-V-Unterstützung des Host-Überwachungs Diensts ermöglicht den virtualisierungsbasierten Schutz der Code Integrität, der möglicherweise mit einigen Geräten nicht kompatibel ist. Wir empfehlen dringend, diese Konfiguration in Ihrem Lab zu testen, bevor Sie diese Funktion aktivieren. Andernfalls kann es zu unerwarteten Fehlern und sogar zu Datenverlusten oder zu einem Bluescreen (STOP-Fehler) kommen.

```
Install-WindowsFeature Hyper-V, HostGuardian -IncludeManagementTools -Restart
```

2. Führen Sie den folgenden Befehl in einer Windows PowerShell-Konsole mit erhöhten Rechten aus, um die Baseline-Richtlinie aufzuzeichnen.

```
Get-HgsAttestationBaselinePolicy -Path 'HWConfig1.tcglog'
```

NOTE

Sie müssen das Flag "-skipvalidation" verwenden, wenn auf dem Referenz Host kein sicherer Start aktiviert ist, ein IOMMU vorhanden ist, die virtualisierungsbasierte Sicherheit aktiviert ist und ausgeführt wird, oder eine Code Integritätsrichtlinie angewendet wird. Diese Überprüfungen sind so konzipiert, dass Sie die Mindestanforderungen für das Ausführen einer abgeschirmten VM auf dem Host kennen. Wenn Sie das Flag "-skipvalidation" verwenden, wird die Ausgabe des Cmdlets nicht geändert. Die Fehler werden lediglich mit einem Fehler verursacht.

3. Stellen Sie die TPM-Baseline (tcglog-Datei) für den HGS-Administrator bereit.
4. Kopieren Sie in der HGS-Domäne die Datei tcglog auf einen HGS-Server, und führen Sie den folgenden Befehl aus. In der Regel benennen Sie die Richtlinie nach der Klasse der Hardware, die Sie repräsentiert (z. b. "Hersteller Modell Revision").

```
Add-HgsAttestationTpmPolicy -Path <Filename>.tcglog -Name '<PolicyName>'
```

Nächster Schritt

[Bestätigen des Nachweises](#)

Erstellen eines Host Schlüssels und Hinzufügen des Schlüssels zu HGS

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019

In diesem Thema wird beschrieben, wie Hyper-V-Hosts mithilfe des Host Schlüssel Nachweis (Schlüssel Modus) auf geschützte Hosts vorbereitet werden. Erstellen Sie ein Host Schlüsselpaar (oder verwenden Sie ein vorhandenes Zertifikat), und fügen Sie die öffentliche Hälfte des Schlüssels zu HGS hinzu.

Erstellen eines Host Schlüssels

1. Installieren Sie Windows Server 2019 auf dem Hyper-V-Host Computer.
2. Installieren Sie die Hyper-v-und Host-Überwachungsfunktionen von Hyper-v:

```
```powershell
Install-WindowsFeature Hyper-V, HostGuardian -IncludeManagementTools -Restart
```
```

3. Generieren Sie automatisch einen Host Schlüssel, oder wählen Sie ein vorhandenes Zertifikat aus. Wenn Sie ein benutzerdefiniertes Zertifikat verwenden, sollte es mindestens einen 2048-Bit-RSA-Schlüssel, eine Clientauthentifizierungs-EKU und die Verwendung von digitalen Signatur Schlüsseln aufweisen.

```
```powershell
Set-HgsClientHostKey
```
```

Alternativ können Sie einen Fingerabdruck angeben, wenn Sie Ihr eigenes Zertifikat verwenden möchten.Alternatively, you can specify a thumbprint if you want to use your own certificate.

Dies kann hilfreich sein, wenn Sie ein Zertifikat für mehrere Computer freigeben möchten, oder wenn Sie ein Zertifikat verwenden möchten, das an ein TPM oder ein HSM gebunden ist.This can be useful if you want to share a certificate across multiple machines, or use a certificate bound to a TPM or an HSM. Hier ist ein Beispiel für das Erstellen eines TPM-gebundenen Zertifikats (das verhindert, dass der private Schlüssel gestohlen und auf einem anderen Computer verwendet wird und nur ein TPM 1,2 erforderlich ist):Here's an example of creating a TPM-bound certificate (which prevents it from having the private key stolen and used on another machine and requires only a TPM 1.2):

```
```powershell
$tpmBoundCert = New-SelfSignedCertificate -Subject "Host Key Attestation ($env:computername)" -Provider "Microsoft Platform Crypto Provider"
Set-HgsClientHostKey -Thumbprint $tpmBoundCert.Thumbprint
```
```

4. Holen Sie sich die öffentliche Hälfte des Schlüssels, der für den HGS-Server bereitgestellt werden soll. Sie können das folgende Cmdlet verwenden oder, wenn Sie das Zertifikat an einem anderen Speicherort gespeichert haben, eine CER-Datei mit der öffentlichen Hälfte des Schlüssels bereitstellen. Beachten Sie, dass wir nur den öffentlichen Schlüssel auf HGS speichern und validieren. Wir behalten keine Zertifikat Informationen bei und überprüfen weder die Zertifikatskette noch das Ablaufdatum.

```
```powershell
Get-HgsClientHostKey -Path "C:\temp\$env:hostname-HostKey.cer"
```
```

5. Kopieren Sie die CER-Datei auf Ihren HGS-Server.

Hinzufügen des Host Schlüssels zum Nachweis Dienst

Dieser Schritt wird auf dem HGS-Server ausgeführt und ermöglicht es dem Host, abgeschirmte VMS auszuführen. Es wird empfohlen, den Namen für den FQDN oder den Ressourcen Bezeichner des Host Computers festzulegen, damit Sie leicht auf den Host, auf dem der Schlüssel installiert ist, verweisen können.

```
Add-HgsAttestationHostKey -Name MyHost01 -Path "C:\temp\MyHost01-HostKey.cer"
```

Nächster Schritt

[Bestätigen, dass Hosts erfolgreich bestätigen können](#)

Siehe auch

- [Bereitstellen des Host-Überwachungs Diensts für geschützte Hosts und abgeschirmte VMS](#)

Erstellen einer Sicherheitsgruppe für geschützte Hosts und Registrieren der Gruppe bei HGS

13.05.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016

IMPORTANT

Der AD-Modus ist ab Windows Server 2019 veraltet. Für Umgebungen, in denen ein TPM-Nachweis nicht möglich ist, konfigurieren Sie den [Host Schlüssel](#) Nachweis. Der Host Schlüssel Nachweis bietet eine ähnliche Garantie für den AD-Modus und ist einfacher einzurichten.

In diesem Thema werden die Zwischenschritte zum Vorbereiten von Hyper-V-Hosts auf überwachte Hosts mithilfe von Administrator vertrauenswürdigen Nachweis (AD-Modus) beschrieben. Bevor Sie diese Schritte ausführen, führen Sie die Schritte unter [Konfigurieren des Fabric-DNS für Hosts aus, die zu überwachte Hosts](#) werden.

Erstellen einer Sicherheitsgruppe und Hinzufügen von Hosts

1. Erstellen Sie eine neue **globale** Sicherheitsgruppe in der Fabric-Domäne, und fügen Sie Hyper-V-Hosts hinzu, auf denen geschützte VMS ausgeführt werden. Starten Sie die Hosts neu, um deren Gruppenmitgliedschaft zu aktualisieren.
2. Verwenden Sie Get-adgroup zum Abrufen der Sicherheits-ID (SID) der Sicherheitsgruppe, und stellen Sie Sie für den HGS-Administrator bereit.

```
Get-ADGroup "Guarded Hosts"
```

```
PS C:\> Get-ADGroup 'Guarded Hosts'

DistinguishedName : CN=Guarded Hosts,CN=Users,DC=contoso,DC=com
GroupCategory     : Security
GroupScope        : Global
Name              : Guarded Hosts
ObjectClass       : group
ObjectGUID        : b00c72cc-69dd-4010-9c97-f31062199f9c
SamAccountName    : Guarded Hosts
SID               : S-1-5-21-947661373-489659989-2802621743-1119
```

Registrieren der SID der Sicherheitsgruppe bei HGS

1. Führen Sie auf einem HGS-Server den folgenden Befehl aus, um die Sicherheitsgruppe bei HGS zu registrieren. Führen Sie den Befehl bei Bedarf erneut für weitere Gruppen aus. Geben Sie einen anzeigen Amen für die Gruppe an. Er muss nicht mit dem Namen der Active Directory Sicherheitsgruppe identisch sein.

```
Add-HgsAttestationHostGroup -Name "<GuardedHostGroup>" -Identifier "<SID>"
```

2. Führen Sie [Get-hgsattestationhostgroup](#) aus, um zu überprüfen, ob die Gruppe hinzugefügt wurde.

Nächster Schritt

[Bestätigen des Nachweises](#)

Siehe auch

- [Bereitstellen des Host-Überwachungsdiensts für überwachte Hosts und abgeschirmte VMs](#)

Bestätigen, dass geschützte Hosts bestätigen können

09.04.2020 • 4 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Ein fabricadministrator muss bestätigen, dass Hyper-V-Hosts als geschützte Hosts ausgeführt werden können. Führen Sie die folgenden Schritte auf mindestens einem überwachten Host aus:

1. Wenn Sie die Hyper-v-Rolle und die Hyper-v-Unterstützung des Host-Überwachungs Diensts noch nicht installiert haben, installieren Sie diese mit dem folgenden Befehl:

```
Install-WindowsFeature Hyper-V, HostGuardian -IncludeManagementTools -Restart
```

2. Stellen Sie sicher, dass der Hyper-V-Host den DNS-Namen des HGS auflösen kann und über die Netzwerk Konnektivität zum Erreichen von Port 80 (oder 443, wenn Sie HTTPS einrichten) auf dem HGS-Server verfügt.
3. Konfigurieren Sie die Schlüsselschutz-und Nachweis-URLs des Hosts:

- **Über Windows PowerShell:** Sie können die Schlüsselschutz-und Nachweis-URLs konfigurieren, indem Sie den folgenden Befehl in einer Windows PowerShell-Konsole mit erhöhten Rechten ausführen. Verwenden Sie für <FQDN>den voll qualifizierten Domänen Namen (Fully Qualified Domain Name, FQDN) Ihres HGS-Clusters (z. b. HGS. Bastion. local), oder bitten Sie den HGS-Administrator, das Cmdlet **Get-hgsserver** auf dem HGS-Server auszuführen, um die URLs abzurufen.

```
Set-HgsClientConfiguration -AttestationServerUrl 'http://<FQDN>/Attestation' -  
KeyProtectionServerUrl 'http://<FQDN>/KeyProtection'
```

Um einen Fall Back-HGS-Server zu konfigurieren, wiederholen Sie diesen Befehl, und geben Sie die Fall Back-URLs für die Schlüsselschutz-und Nachweis Dienste an. Weitere Informationen finden Sie unter [Fall Back Konfiguration](#).

- **Über VMM:** Wenn Sie System Center 2016-Virtual Machine Manager (VMM) verwenden, können Sie die URLs für den Nachweis und den Schlüsselschutz in VMM konfigurieren. Weitere Informationen finden Sie unter [Konfigurieren globaler HGS-Einstellungen](#) in Bereitstellen von überwachten Hosts in VMM.

Hinweise

- Wenn der HGS-Administrator [https auf dem HGS-Server aktiviert](#)hat, starten Sie die URLs mit `https://`.
- Wenn der HGS-Administrator HTTPS auf dem HGS-Server aktiviert und ein selbst signiertes Zertifikat verwendet hat, müssen Sie das Zertifikat in den Speicher vertrauenswürdiger Stamm Zertifizierungsstellen auf jedem Host importieren. Führen Sie hierzu den folgenden Befehl auf jedem Host aus:

```
PowerShell Import-Certificate -FilePath "C:\temp\HttpsCertificate.cer" -CertStoreLocation  
Cert:\LocalMachine\Root
```

- Wenn Sie den HGS-Client für die Verwendung von HTTPS konfiguriert und TLS 1,0 systemwide deaktiviert haben, finden Sie in unserem [modernen TLS-Leitfaden](#) Weitere Informationen.

4. Führen Sie den folgenden Befehl aus, um einen Nachweis Versuch auf dem Host zu initiieren und den Nachweis Status anzuzeigen:

```
Get-HgsClientConfiguration
```

Die Ausgabe des Befehls gibt an, ob der Host den Nachweis überschritten hat und nun geschützt ist. Wenn `IsHostGuarded` nicht "true" zurückgibt, können Sie das HGS-Diagnosetool "[Get-hgstrace](#)" ausführen, um dies zu untersuchen. Um die Diagnose auszuführen, geben Sie den folgenden Befehl in einer Windows PowerShell-Eingabeaufforderung mit erhöhten Rechten auf dem Host ein:

```
Get-HgsTrace -RunDiagnostics -Detailed
```

IMPORTANT

Wenn Sie Windows Server 2019 oder Windows 10, Version 1809, verwenden und Code Integritäts Richtlinien verwenden, wird `Get-HgsTrace` einen Fehler für die **aktive Diagnose der Code Integritätsrichtlinie** zurückgeben. Sie können dieses Ergebnis gefahrlos ignorieren, wenn es die einzige Fehlerdiagnose ist.

Nächster Schritt

[Bereitstellen von abgeschirmten VMs](#)

Siehe auch

- [Bereitstellen des Host-Überwachungs Diensts \(HGS\)](#)
- [Bereitstellen von abgeschirmten VMs](#)

Bereitstellen von abgeschirmten VMs

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

In den folgenden Themen wird beschrieben, wie ein Mandant mit abgeschirmten VMS arbeiten kann.

1. Optionale [Erstellen Sie einen Windows-Vorlagen](#) Datenträger, oder [Erstellen Sie einen Linux-Vorlagen](#) Der Vorlagen Datenträger kann entweder vom Mandanten oder vom hostingdienstanbieter erstellt werden.
2. Optionale [Konvertieren einer vorhandenen Windows-VM in eine abgeschirmte VM](#)
3. [Erstellen Sie Schutz Daten, um eine abgeschirmte VM zu definieren.](#)

Eine Beschreibung und ein Diagramm für eine geschützte Datendatei finden [Sie unter Was sind geschützte Daten? und warum ist es notwendig?](#)

Informationen zum Erstellen einer Antwortdatei, die in eine geschützte Datendatei aufgenommen werden soll, finden Sie unter [abgeschirmte VMS: Generieren einer Antwortdatei mithilfe der New-shieldingdatabaseantwortungsdateifunktion.](#)

4. Erstellen einer abgeschirmten VM:
 - Verwenden von **Windows Azure Pack**: bereitstellen [einer abgeschirmten VM mithilfe Windows Azure Pack](#)
 - Verwenden von **Virtual Machine Manager**: bereitstellen [einer abgeschirmten VM mithilfe Virtual Machine Manager](#)

Nächster Schritt

[Erstellen einer abgeschirmten VM-Vorlage](#)

Siehe auch

- [Geschütztes Fabric und abgeschirmte VMs](#)

Erstellen eines Datenträgers für eine geschützte Windows-VM-Vorlage

09.04.2020 • 20 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2019

Wie bei regulären virtuellen Computern können Sie eine VM-Vorlage erstellen (z. b. eine [VM-Vorlage in Virtual Machine Manager \(VMM\)](#)), damit Mandanten und Administratoren mithilfe eines Vorlagen Datenträgers problemlos neue VMS im Fabric bereitstellen können. Da abgeschirmte VMS sicherheitsrelevante Ressourcen sind, sind zusätzliche Schritte erforderlich, um eine VM-Vorlage zu erstellen, die Schutz unterstützt. In diesem Thema werden die Schritte zum Erstellen eines geschützten Vorlagen Datenträgers und einer VM-Vorlage in VMM behandelt.

Informationen dazu, wie sich dieses Thema in den Gesamtprozess der Bereitstellung von abgeschirmten VMS einfügt, finden Sie unter [Hosten von Dienst Anbietern Konfigurationsschritte für geschützte Hosts und abgeschirmte VMS](#).

Vorbereiten einer vhdx-Betriebssystem Datei

Bereiten Sie zuerst einen Betriebssystem Datenträger vor, den Sie dann mit dem Assistenten zum Erstellen einer abgeschirmten Vorlage ausführen. Dieser Datenträger wird als Betriebssystem Datenträger in den virtuellen Computern Ihres Mandanten verwendet. Zum Erstellen dieses Datenträgers können Sie beliebige vorhandene Tools verwenden, z. b. Microsoft Desktop Image Service Manager (MAGE), oder Sie können manuell einen virtuellen Computer mit einer leeren vhdx einrichten und das Betriebssystem auf diesem Datenträger installieren. Beim Einrichten des Datenträgers müssen die folgenden Anforderungen erfüllt werden, die für die Generation 2 und/oder abgeschirmte VMS spezifisch sind:

| ANFORDERUNG FÜR VHDX | GRUND |
|---|---|
| Muss ein GPT-Datenträger (GUID-Partitionstabelle) sein. | Erforderlich für virtuelle Computer der Generation 2 zur Unterstützung von UEFI |
| Der Datenträgertyp muss Standard und nicht dynamisch sein .
Hinweis: Dies bezieht sich auf den Typ des logischen Datenträgers, nicht auf das von Hyper-V unterstützte "dynamisch erweiterbare" vhdx-Feature. | BitLocker unterstützt keine dynamischen Datenträger. |
| Der Datenträger verfügt über mindestens zwei Partitionen. Eine Partition muss das Laufwerk enthalten, auf dem Windows installiert ist. Dies ist das Laufwerk, das von BitLocker verschlüsselt wird. Die andere Partition ist die aktive Partition, die den Bootloader enthält und unverschlüsselt bleibt, damit der Computer gestartet werden kann. | Für BitLocker erforderlich |
| Dateisystem ist NTFS | Für BitLocker erforderlich |

| ANFORDERUNG FÜR VHDX | GRUND |
|--|---|
| Das auf der vhdx installierte Betriebssystem ist einer der folgenden:
-Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012
-Windows 10, Windows 8.1, Windows 8 | Erforderlich zur Unterstützung virtueller Maschinen der Generation 2 und der Microsoft-Vorlage für den sicheren Start |
| Das Betriebssystem muss generalisiert sein (führen Sie "sysprep. exe" aus). | Die Vorlagen Bereitstellung umfasst spezialisierte VMs für die Arbeitsauslastung eines bestimmten Mandanten. |

NOTE

Wenn Sie VMM verwenden, kopieren Sie den Vorlagen Datenträger in dieser Phase nicht in die VMM-Bibliothek.

Ausführen von Windows Update auf dem Vorlagen Betriebssystem

Vergewissern Sie sich auf dem Vorlagen Datenträger, dass alle aktuellen Windows-Updates auf dem Betriebssystem installiert sind. Kürzlich veröffentlichte Updates verbessern die Zuverlässigkeit des End-to-End-Schutz Vorgangs. Dies ist ein Prozess, der möglicherweise nicht abgeschlossen wird, wenn das Vorlagen Betriebssystem nicht auf dem neuesten Stand ist.

Vorbereiten und schützen der vhdx-Datei mit dem Vorlagen Datenträger-Assistenten

Um einen Vorlagen Datenträger mit abgeschirmten VMS zu verwenden, muss der Datenträger mithilfe des Assistenten für die Datenträger Erstellung für abgeschirmte Vorlagen mit BitLocker vorbereitet und verschlüsselt werden. Dieser Assistent generiert einen Hash für den Datenträger und fügt ihn einem volumesignaturkatalog (VSC) hinzu. Der VSC wird mit einem von Ihnen angegebenen Zertifikat signiert und während des Bereitstellungs Prozesses verwendet, um sicherzustellen, dass der Datenträger, der für einen Mandanten bereitgestellt wird, nicht geändert oder durch einen Datenträger ersetzt wurde, dem der Mandant nicht vertraut. Schließlich wird BitLocker auf dem Betriebssystem des Datenträgers installiert (sofern es noch nicht vorhanden ist), um den Datenträger für die Verschlüsselung während der VM-Bereitstellung vorzubereiten.

NOTE

Der Vorlagen Datenträger-Assistent ändert den Vorlagen Datenträger, den Sie direkt angeben. Sie sollten eine Kopie der ungeschützten vhdx-Datei erstellen, bevor Sie den Assistenten ausführen, um die Datenträger zu einem späteren Zeitpunkt zu aktualisieren. Sie können einen Datenträger, der mit dem Vorlagen Datenträger-Assistenten geschützt wurde, nicht ändern.

Führen Sie die folgenden Schritte auf einem Computer aus, auf dem Windows Server 2016, Windows 10 (mit Remote Server-Verwaltungs Tools, RSAT installiert) oder höher ausgeführt wird (es muss sich nicht um einen überwachten Host oder VMM-Server handeln):

1. Kopieren Sie die in [Vorbereiten einer Betriebssystem-vhdx](#) erstellte generalisierte vhdx auf den Server, sofern diese nicht bereits vorhanden ist.
2. Um den Server lokal zu verwalten, installieren Sie das Feature der **abgeschirmten VM-Tools** von **Remoteserver-Verwaltungstools** auf dem Server.

```
Install-WindowsFeature RSAT-Shielded-VM-Tools -Restart
```

Sie können den Server auch über einen Client Computer verwalten, auf dem Sie die [Windows 10-Remoteserver-Verwaltungstools](#) installiert haben.

3. Abrufen oder Erstellen eines Zertifikats zum Signieren des VSC für die vhdx-Datei, die als Vorlagen Datenträger für neue abgeschirmte VMS verwendet wird. Details zu diesem Zertifikat werden den Mandanten angezeigt, wenn Sie Ihre geschützten Datendateien erstellen und die Datenträger autorisiert, denen Sie vertrauen. Daher ist es wichtig, dass Sie dieses Zertifikat von einer Zertifizierungsstelle abrufen, die von Ihnen und ihren Mandanten als nicht vertrauenswürdig eingestuft wird. In Unternehmens Szenarios, in denen Sie sowohl der Host als auch der Mandant sind, sollten Sie das Zertifikat aus Ihrer PKI ausgeben.

Wenn Sie eine Testumgebung einrichten und nur ein selbst signiertes Zertifikat verwenden möchten, um den Vorlagen Datenträger vorzubereiten, führen Sie einen Befehl aus, der dem folgenden ähnelt:

```
New-SelfSignedCertificate -DnsName publisher.fabrikam.com
```

4. Starten Sie den Vorlagen Datenträger- **Assistenten** im Ordner "**Verwaltung**" im Startmenü, oder geben Sie "**templatediskwizard.exe**" an einer Eingabeaufforderung ein.
5. Klicken Sie auf der Seite **Zertifikat** auf **Durchsuchen**, um eine Liste mit Zertifikaten anzuzeigen. Wählen Sie das Zertifikat aus, mit dem die Datenträger Vorlage vorbereitet werden soll. Klicken Sie auf **OK** und dann auf **Weiter**.
6. Klicken Sie auf der Seite virtueller Datenträger auf **Durchsuchen**, um das vhdx auszuwählen, das Sie vorbereitet haben, und klicken Sie dann auf **weiter**.
7. Geben Sie auf der Seite Signatur Katalog einen anzeigen **Amen** und eine **Version** des Datenträgers an. Diese Felder sind vorhanden, damit Sie den Datenträger nach der Vorbereitung identifizieren können.

Beispielsweise können Sie **disk name** für den Datenträger Namen *WS2016* und für **Version**, *1.0.0.0* eingeben.

8. Überprüfen Sie Ihre Auswahl auf der Seite Einstellungen überprüfen des Assistenten. Wenn Sie auf **generieren** klicken, aktiviert der Assistent BitLocker auf dem Vorlagen Datenträger, berechnet den Hash des Datenträgers und erstellt den volumensignaturkatalog, der in den vhdx-Metadaten gespeichert ist.

Warten Sie, bis der Vorbereitungs Vorgang abgeschlossen ist, bevor Sie versuchen, den Vorlagen Datenträger zu starten. Der Vorgang kann je nach Größe des Datenträgers einige Zeit in Anspruch nehmen.

IMPORTANT

Vorlagen Datenträger können nur mit dem sicheren geschützten VM-Bereitstellungs Prozess verwendet werden. Der Versuch, einen regulären virtuellen Computer mit einem Vorlagen Datenträger zu starten, führt wahrscheinlich zu einem Fehler beim Abbrechen (blauer Bildschirm) und wird nicht unterstützt.

9. Auf der Seite **Zusammenfassung** werden Informationen zur Datenträger Vorlage, zum Zertifikat, das zum Signieren des VSC und zum Aussteller des Zertifikats verwendet wird, angezeigt. Klicken Sie auf **Schließen**, um den Assistenten zu beenden.

Wenn Sie VMM verwenden, führen Sie die Schritte in den restlichen Abschnitten in diesem Thema aus, um einen Vorlagen Datenträger in eine geschützte VM-Vorlage in VMM einzubinden.

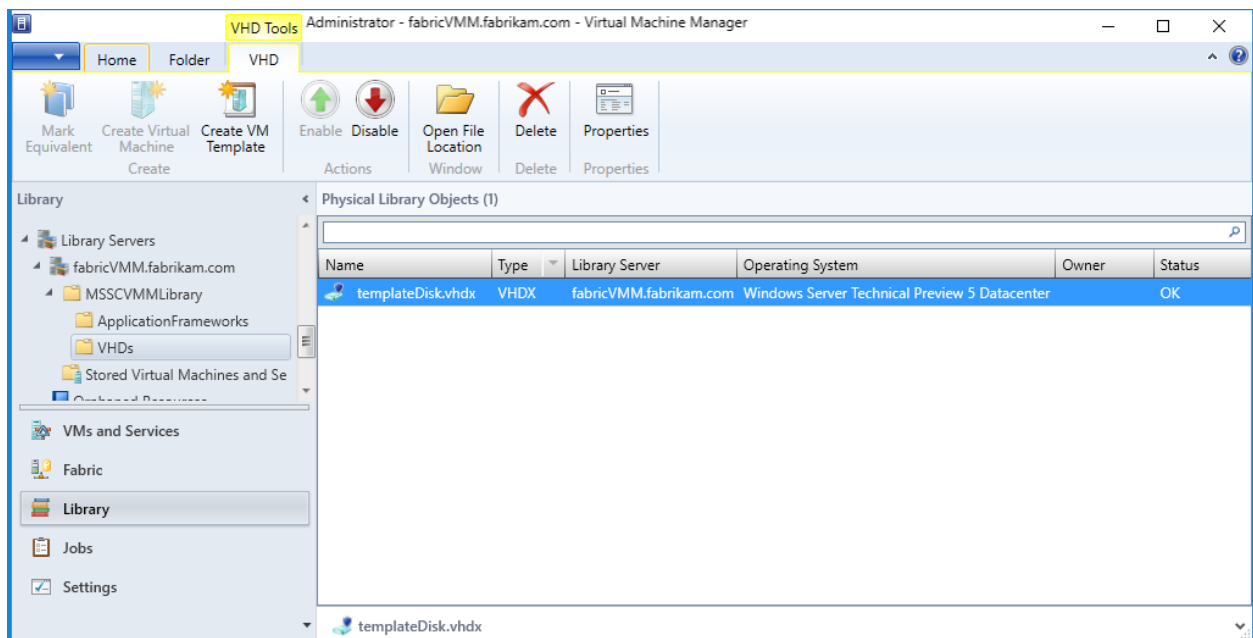
Kopieren Sie den Vorlagen Datenträger in die VMM-Bibliothek

Wenn Sie VMM verwenden, müssen Sie nach dem Erstellen eines Vorlagen Datenträgers diese Datei in eine

VMM-Bibliothek freigabe kopieren, damit Hosts den Datenträger herunterladen und verwenden können, wenn Sie neue VMs bereitstellen. Verwenden Sie das folgende Verfahren, um den Vorlagen Datenträger in die VMM-Bibliothek zu kopieren und dann die Bibliothek zu aktualisieren.

1. Kopieren Sie die vhdx-Datei in den Ordner der VMM-Bibliothek freigabe. Wenn Sie die VMM-Standardkonfiguration verwendet haben, kopieren Sie den Vorlagen Datenträger in \\msscvmmlibrary\vhds.
2. Aktualisieren Sie den Bibliothek Server. Öffnen Sie den Arbeitsbereich **Bibliothek**, erweitern Sie **Bibliothek Server**, klicken Sie mit der rechten Maustaste auf den Bibliothek Server, den Sie aktualisieren möchten, und klicken Sie auf **Aktualisieren**.
3. Als Nächstes stellen Sie VMM Informationen zum Betriebssystem bereit, das auf dem Vorlagen Datenträger installiert ist:
 - a. Suchen Sie den neu importierten Vorlagen Datenträger auf dem Bibliothek Server im Arbeitsbereich **Bibliothek**.
 - b. Klicken Sie mit der rechten Maustaste auf den Datenträger und dann auf **Eigenschaften**.
 - c. Erweitern Sie unter **Betriebssystem** die Liste, und wählen Sie das Betriebssystem aus, das auf dem Datenträger installiert ist. Die Auswahl eines Betriebssystems weist VMM darauf hin, dass die vhdx nicht leer ist.
 - d. Klicken Sie auf **OK**.

Das kleine Schild Symbol neben dem Namen des Datenträgers bezeichnet den Datenträger als vorbereiteten Vorlagen Datenträger für geschützte VMS. Sie können auch mit der rechten Maustaste auf die Spaltenüberschriften klicken und die **geschützte** Spalte umschalten, um eine Textdarstellung anzuzeigen, die angibt, ob ein Datenträger für reguläre oder abgeschirmte VM-bereit Stellungen vorgesehen ist.



Erstellen der abgeschirmten VM-Vorlage in VMM mithilfe des vorbereiteten Vorlagen Datenträgers

Mit einem vorbereiteten Vorlagen Datenträger in der VMM-Bibliothek können Sie eine VM-Vorlage für abgeschirmte VMS erstellen. VM-Vorlagen für abgeschirmte VMS unterscheiden sich geringfügig von herkömmlichen VM-Vorlagen dahin, dass bestimmte Einstellungen fest sind (VM der Generation 2, UEFI und sicherer Start aktiviert usw.) und andere nicht verfügbar sind (die Anpassung von Mandanten ist auf einige wenige, ausgewählte Eigenschaften der VM beschränkt). Führen Sie die folgenden Schritte aus, um die VM-

Vorlage zu erstellen:

1. Klicken Sie im Arbeitsbereich **Bibliothek** oben auf der Registerkarte Start auf **VM-Vorlage erstellen**.
2. Klicken Sie auf der Seite **Quelle auswählen** auf **Vorhandene VM-Vorlage oder in der Bibliothek gespeicherte virtuelle Festplatte verwenden** und dann auf **Durchsuchen**.
3. Wählen Sie im angezeigten Fenster einen vorbereiteten Vorlagen Datenträger aus der VMM-Bibliothek aus. Um leichter festzustellen, welche Datenträger vorbereitet werden, klicken Sie mit der rechten Maustaste auf einen Spaltenheader, und aktivieren Sie die **geschützte** Spalte. Klicken Sie auf **OK** und dann **weiter**.
4. Geben Sie einen VM-Vorlagen Namen und optional eine Beschreibung ein, und klicken Sie dann auf **weiter**.
5. Geben Sie auf der Seite **Hardware konfigurieren** die Funktionen der virtuellen Computer an, die aus dieser Vorlage erstellt wurden. Stellen Sie sicher, dass mindestens eine NIC für die VM-Vorlage verfügbar und konfiguriert ist. Die einzige Möglichkeit für einen Mandanten, eine Verbindung mit einer abgeschirmten VM herzustellen, ist die Remotedesktopverbindung, Windows-Remoteverwaltung oder anderen vorkonfigurierten Remote Verwaltungs Tools, die über Netzwerkprotokolle arbeiten.

Wenn Sie statische IP-Pools in VMM nutzen möchten, anstatt einen DHCP-Server im Mandanten Netzwerk ausführen zu müssen, müssen Sie Ihre Mandanten für diese Konfiguration benachrichtigen. Wenn ein Mandant seine Schutz Datendatei bereitstellt, die die Datei für die unbeaufsichtigte Installation für VMM enthält, muss er spezielle Platzhalter Werte für die Informationen des statischen IP-Pools angeben. Weitere Informationen zu VMM-Platzhaltern in Dateien für die unbeaufsichtigte Installation von Mandanten finden Sie unter [Erstellen einer Antwortdatei](#).

6. Auf der Seite **Betriebs System konfigurieren** werden von VMM nur einige Optionen für abgeschirmte VMS angezeigt, einschließlich der Product Key, der Zeitzone und des Computer namens. Einige sichere Informationen, z. b. das Administrator Kennwort und der Domänen Name, werden vom Mandanten über eine geschützte Datendatei () angegeben. PDK-Datei).

NOTE

Wenn Sie einen Product Key auf dieser Seite angeben, stellen Sie sicher, dass er für das Betriebssystem auf dem Vorlagen Datenträger gültig ist. Wenn eine falsche Product Key verwendet wird, tritt bei der VM-Erstellung ein Fehler auf.

Nachdem die Vorlage erstellt wurde, können Mandanten Sie zum Erstellen neuer virtueller Maschinen verwenden. Sie müssen überprüfen, ob es sich bei der VM-Vorlage um eine der für die Mandantenadministrator-Benutzerrolle verfügbaren Ressourcen handelt (in VMM befinden sich Benutzer Rollen im Arbeitsbereich "**Einstellungen**").

Vorbereiten und schützen der vhdx-Datei mithilfe von PowerShell

Als Alternative zum Ausführen des Assistenten für Vorlagen Datenträger können Sie den Vorlagen Datenträger und das Zertifikat auf einen Computer mit RSAT kopieren und [Protect-templatedisk](#) ausführen, um den Signatur Prozess zu initiieren. Im folgenden Beispiel werden der Name und die Versionsinformationen verwendet, die von den Parametern *templatename* und *Version* angegeben werden. Die vhdx, die Sie dem `-Path` -Parameter bereitstellen, wird mit dem aktualisierten Vorlagen Datenträger überschrieben. Stellen Sie daher sicher, dass Sie vor dem Ausführen des Befehls eine Kopie erstellen

```
# Replace "THUMBPRINT" with the thumbprint of your template disk signing certificate in the line below
$certificate = Get-Item Cert:\LocalMachine\My\THUMBPRINT

Protect-TemplateDisk -Certificate $certificate -Path "WindowsServer2019-ShieldedTemplate.vhdx" -TemplateName
"Windows Server 2019" -Version 1.0.0.0
```

Der Vorlagen Datenträger kann jetzt zum Bereitstellen von abgeschirmten VMS verwendet werden. Wenn Sie System Center Virtual Machine Manager zum Bereitstellen Ihrer VM verwenden, können Sie jetzt die vhdx-Datei in die VMM-Bibliothek kopieren.

Möglicherweise möchten Sie auch den volumesignaturkatalog aus der vhdx-Datei extrahieren. Diese Datei wird verwendet, um Informationen über das Signaturzertifikat, den Datenträger Namen und die Version für die VM-Besitzer bereitzustellen, die Ihre Vorlage verwenden möchten. Sie müssen diese Datei in den Assistenten für die Schutz Datendatei importieren, um Sie zu autorisieren, den Vorlagen Autor im Besitz des Signatur Zertifikats, um diesen und zukünftige Vorlagen Datenträger zu erstellen.

Führen Sie den folgenden Befehl in PowerShell aus, um den volumesignaturkatalog zu extrahieren:

```
Save-VolumeSignatureCatalog -TemplateDiskPath 'C:\temp\MyLinuxTemplate.vhdx' -VolumeSignatureCatalogPath
'C:\temp\MyLinuxTemplate.vsc'
```

Nächster Schritt

[Erstellen einer Schutz Datendatei](#)

Siehe auch

- [Konfigurationsschritte des hostingdiensteanbieters für geschützte Hosts und abgeschirmte VMS](#)
- [Geschütztes Fabric und abgeschirmte VMs](#)

Erstellen eines virtuellen Linux-VM-Vorlagen Datenträgers

09.04.2020 • 15 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal),

In diesem Thema wird erläutert, wie ein Vorlagen Datenträger für abgeschirmte Linux-VMs vorbereitet wird, mit denen eine oder mehrere Mandanten-VMS instanziiert werden können.

Erforderliche Komponenten

Zum Vorbereiten und Testen einer abgeschirmten Linux-VM benötigen Sie die folgenden verfügbaren Ressourcen:

- Ein Server mit Virtualisierungsplattformen, auf denen Windows Server, Version 1709 oder höher, ausgeführt wird
- Ein zweiter Computer (Windows 10 oder Windows Server 2016), der Hyper-V-Manager zum Herstellen einer Verbindung mit der Konsole des laufenden virtuellen Computers ausführen muss
- Ein ISO-Abbild für einen der unterstützten Linux-VM-Betriebssysteme:
 - Ubuntu 16,04 LTS mit dem 4,4-Kernel
 - Red Hat Enterprise Linux 7.3
 - SUSE Linux Enterprise Server 12 Service Pack 2
- Internet Zugriff zum Herunterladen des lsvmttools-Pakets und der Betriebssystemupdates

IMPORTANT

Neuere Versionen der vorangehenden Linux-Betriebssysteme können einen bekannten TPM-Treiber Fehler enthalten, der verhindert, dass Sie als abgeschirmte VMS erfolgreich bereitgestellt werden. Es wird nicht empfohlen, Ihre Vorlagen oder abgeschirmten VMS auf eine neuere Version zu aktualisieren, bis eine Korrektur vorliegt. Die Liste der oben unterstützten Betriebssysteme wird aktualisiert, wenn die Updates öffentlich gemacht werden.

Vorbereiten einer Linux-VM

Abgeschirmte VMS werden aus sicheren Vorlagen Datenträgern erstellt. Vorlagen Datenträger enthalten das Betriebssystem für den virtuellen Computer und die Metadaten, einschließlich einer digitalen Signatur der/Boot- und/Root-Partitionen, um sicherzustellen, dass die wesentlichen Betriebssystemkomponenten vor der Bereitstellung nicht geändert

Um einen Vorlagen Datenträger zu erstellen, müssen Sie zunächst eine reguläre (nicht genehmigte) VM erstellen, die Sie als Basis Image für künftige abgeschirmte VMS vorbereiten. Die von Ihnen installierte Software und Konfigurationsänderungen, die Sie an diesem virtuellen Computer vornehmen, gelten für alle abgeschirmten VMS, die auf dieser Vorlage erstellt werden. Diese Schritte führen Sie durch die Mindestanforderungen für eine Linux-VM, die für die Vorlagen-atisierung bereit steht.

NOTE

Die Linux-Datenträger Verschlüsselung wird konfiguriert, wenn der Datenträger partitioniert ist. Dies bedeutet, dass Sie einen neuen virtuellen Computer erstellen müssen, der mithilfe von dm-crypt vorverschlüsselt ist, um einen Linux-Vorlagen Datenträger für geschützte VM zu erstellen

1. Stellen Sie auf dem Virtualisierungsserver sicher, dass Hyper-v und die Hyper-v-Unterstützung für den Host-Überwachungsdienst installiert werden, indem Sie die folgenden Befehle in einer PowerShell-Konsole mit erhöhten

```
Install-WindowsFeature Hyper-V, HostGuardian -IncludeManagementTools -Restart
```

2. Laden Sie das ISO-Abbild von einer vertrauenswürdigen Quelle herunter, und speichern Sie es auf Ihrem Virtualisierungsserver oder auf einer Dateifreigabe, auf die der Virtualisierungsserver
3. Installieren Sie auf dem Verwaltungs Computer, auf dem Windows Server Version 1709 ausgeführt wird, den geschützten VM-Remoteserver-Verwaltungstools, indem Sie den folgenden Befehl ausführen:

```
Install-WindowsFeature RSAT-Shielded-VM-Tools
```

4. Öffnen Sie den **Hyper-V-Manager** auf dem Verwaltungs Computer, und stellen Sie eine Verbindung mit dem Virtualisierungsserver. Klicken Sie hierzu auf "Verbindung mit Server herstellen...". Klicken Sie im Aktionsbereich oder mit der rechten Maustaste auf Hyper-V-Manager, und wählen Sie "Verbindung mit Server herstellen..." aus. Geben Sie den DNS-Namen für den Hyper-V-Server und ggf. die Anmeldeinformationen an, die zum Herstellen einer Verbindung erforderlich sind.
5. Konfigurieren Sie mit dem Hyper-V-Manager [einen externen Switch](#) auf dem Virtualisierungsserver, damit die Linux-VM auf das Internet zugreifen kann, um Updates abzurufen.
6. Erstellen Sie als nächstes einen neuen virtuellen Computer, auf dem das Linux-Betriebssystem installiert werden soll. Klicken Sie im Aktionsbereich auf **neu > virtuellen Computer**, um den Assistenten zu aktivieren. Geben Sie einen anzeigen Namen für den virtuellen Computer an, z. b. "Pre--Vorlagen-Linux", und klicken Sie auf **weiter**.
7. Wählen Sie auf der zweiten Seite des Assistenten **Generation 2** aus, um sicherzustellen, dass die VM mit einem UEFI-basierten firmwareprofil bereitgestellt wird.
8. Vervollständigen Sie den Rest des Assistenten gemäß Ihren Einstellungen. Verwenden Sie für diese VM keinen differenzierenden Datenträger. für geschützte VM-Vorlagen Datenträger können keine differenzierenden Datenträger Verbinden Sie schließlich das ISO-Abbild, das Sie zuvor heruntergeladen haben, mit dem virtuellen DVD-Laufwerk für diese VM, damit Sie das Betriebssystem installieren können.
9. Wählen Sie im Hyper-V-Manager den neu erstellten virtuellen Computer aus, und klicken Sie im Aktionsbereich auf **verbinden...**, um ihn an eine virtuelle Konsole der VM anzufügen. Klicken Sie im angezeigten Fenster auf **Start**, um den virtuellen Computer zu aktivieren.
10. Durchlaufen Sie den Setup Vorgang für die ausgewählte Linux-Distribution. Obwohl jede Linux-Distribution einen anderen Setup-Assistenten verwendet, müssen die folgenden Anforderungen für VMS erfüllt sein, die zu Linux-Vorlagen Datenträger für virtuelle Computer werden.
 - Der Datenträger muss mithilfe des GPT-Layouts (GUID-Partitionstabelle) partitioniert werden.
 - Die Stamm Partition muss mit dm-crypt verschlüsselt werden. Die Passphrase sollte auf **Passphrase** (nur Kleinbuchstaben) festgelegt werden. Diese Passphrase wird zufällig erstellt, und die Partition wird neu verschlüsselt, wenn eine abgeschirmte VM bereitgestellt wird.

- Die Start Partition muss das **ext2** -Dateisystem verwenden.

11. Nachdem das Linux-Betriebssystem vollständig gestartet wurde und Sie sich angemeldet haben, wird empfohlen, den Linux-virtuellen Kernel und zugehörige Hyper-V-Integrations Dienst Pakete zu installieren. Außerdem sollten Sie einen SSH-Server oder ein anderes Remote Verwaltungs Tool installieren, um auf die VM zuzugreifen, nachdem Sie geschützt wurde.

Führen Sie unter Ubuntu den folgenden Befehl aus, um diese Komponenten zu installieren:

```
sudo apt-get install linux-virtual linux-tools-virtual linux-cloud-tools-virtual linux-image-extra-virtual openssh-server
```

Führen Sie unter RHEL stattdessen den folgenden Befehl aus:

```
sudo yum install hyperv-daemons openssh-server
sudo service sshd start
```

Führen Sie unter SLES den folgenden Befehl aus:

```
sudo zypper install hyper-v
sudo chkconfig hv_kvp_daemon on
sudo systemctl enable sshd
```

12. Konfigurieren Sie das Linux-Betriebssystem wie gewünscht. Jede Software, die Sie installieren, Benutzerkonten, die Sie hinzufügen, und von Ihnen vorgenommene systemweiten Konfigurationsänderungen gelten für alle zukünftigen virtuellen Computer, die auf dieser Vorlagen Datenträger Vermeiden Sie, geheime oder unnötige Pakete auf dem Datenträger zu speichern.
13. Wenn Sie beabsichtigen, System Center Virtual Machine Manager für die Bereitstellung Ihrer VMS zu verwenden, installieren Sie den VMM-Gast-Agent, damit VMM das Betriebssystem während der VM-Bereitstellung spezialisiert. Die Spezialisierung ermöglicht die sichere Einrichtung jeder VM mit unterschiedlichen Benutzern und SSH-Schlüsseln, Netzwerkkonfigurationen und benutzerdefinierten Einrichtungsschritten. Erfahren Sie, wie Sie [den VMM-Gast-Agent](#) in der VMM-Dokumentation abrufen und installieren.
14. [Fügen Sie als nächstes das Microsoft Linux-Softwarerepository Ihrem Paket-Manager hinzu.](#)
15. Installieren Sie mithilfe des Paket-Managers das lsvmtools-Paket, das die Linux-Shim für abgeschirmte VM-Bootloader, Bereitstellungs Komponenten und das Tool zur Datenträger Vorbereitung enthält.

```
# Ubuntu 16.04
sudo apt-get install lsvmtools

# SLES 12 SP2
sudo zypper install lsvmtools

# RHEL 7.3
sudo yum install lsvmtools
```

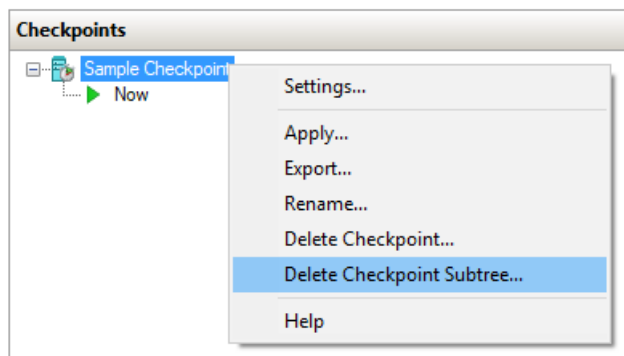
16. Wenn Sie die Anpassung des Linux-Betriebssystems abgeschlossen haben, suchen Sie das Installationsprogramm lsvmprep auf dem System, und führen Sie es aus.

```
# The path below may change based on the version of lsvmprep installed
# Run "find /opt -name lsvmprep" to locate the lsvmprep executable
sudo /opt/lsvmtools-1.0.0-x86-64/lsvmprep
```


17. Fahren Sie Ihren virtuellen Computer herunter.

18. Wenn Sie Prüfpunkte Ihres virtuellen Computers (einschließlich automatischer Prüfpunkte, die von Hyper-V mit dem Windows 10 Fall Creators Update erstellt wurden) vorgenommen haben, achten Sie darauf, dass Sie Sie löschen, bevor Sie fortfahren. Prüfpunkte erstellen differenzierende Datenträger (.avhdx), die vom Vorlagen-Assistenten für Vorlagen nicht unterstützt werden.

Um Prüfpunkte zu löschen, öffnen Sie den **Hyper-V-Manager**, wählen Sie den virtuellen Computer aus, **Klicken Sie mit der rechten Maustaste** auf den obersten Prüfpunkt im Bereich Prüfpunkte, und klicken Sie dann auf Prüfpunkt



Schützen des Vorlagen Datenträgers

Der virtuelle Computer, den Sie im vorherigen Abschnitt vorbereitet haben, ist fast bereit für die Verwendung als Vorlage für abgeschirmte Linux-VM-Vorlagen. Der letzte Schritt besteht darin, den Datenträger mit dem datenträgerdatenträger-Assistenten auszuführen, der den aktuellen Zustand der Stamm- und Start Partitionen Hashs und digital signiert. Der Hash und die digitale Signatur werden überprüft, wenn eine abgeschirmte VM bereitgestellt wird, um sicherzustellen, dass keine nicht autorisierten Änderungen an den beiden Partitionen zwischen der Vorlagen Erstellung und der Bereitstellung vorgenommen wurden.

Abrufen eines Zertifikats zum Signieren des Datenträgers

Um die Datenträger Messungen Digital zu signieren, müssen Sie auf dem Computer, auf dem Sie den Vorlagen Datenträger-Assistenten ausführen werden, ein Zertifikat abrufen. Das Zertifikat muss die folgenden Anforderungen erfüllen:

| ZERTIFIKAT EIGENSCHAFT | ERFORDERLICHER WERT |
|-------------------------|---------------------|
| Schlüssel Algorithmus | RSA |
| Minimale Schlüsselgröße | 2.048 Bits |
| Signatur Algorithmus | SHA256 (empfohlen) |
| Schlüsselverwendung | Digitale Signatur |

Details zu diesem Zertifikat werden den Mandanten angezeigt, wenn Sie Ihre geschützten Datendateien erstellen und die Datenträger autorisiert, denen Sie vertrauen. Daher ist es wichtig, dass Sie dieses Zertifikat von einer Zertifizierungsstelle abrufen, die von Ihnen und ihren Mandanten als nicht vertrauenswürdig eingestuft wird. In Unternehmens Szenarios, in denen Sie sowohl der Host als auch der Mandant sind, sollten Sie dieses Zertifikat von Ihrer Unternehmens Zertifizierungsstelle ausgeben. Schützen Sie dieses Zertifikat sorgfältig, da jeder, der dieses Zertifikat besitzt, neue Vorlagen Datenträger erstellen kann, die mit dem authentischen Datenträger vertrauenswürdig sind.

In einer Testumgebung können Sie mit dem folgenden PowerShell-Befehl ein selbst signiertes Zertifikat erstellen:

```
New-SelfSignedCertificate -Subject "CN=Linux Shielded VM Template Disk Signing Certificate"
```

Verarbeiten des Datenträgers mit dem Datenträger-Assistenten-Cmdlet

Kopieren Sie den Vorlagen Datenträger und das Zertifikat auf einen Computer unter Windows Server, Version 1709, und führen Sie dann die folgenden Befehle aus, um den Signatur Prozess zu initiieren. Die vhd, die Sie dem `-Path` -Parameter bereitstellen, wird mit dem aktualisierten Vorlagen Datenträger überschrieben. Stellen Sie daher sicher, dass Sie vor dem Ausführen des Befehls eine Kopie erstellen.

IMPORTANT

Der Remoteserver-Verwaltungstools, der unter Windows Server 2016 oder Windows 10 verfügbar ist, kann nicht verwendet werden, um einen Linux-Vorlagen Datenträger für geschützte Verwenden Sie das Cmdlet "[Protect-templatedisk](#)", das unter Windows Server, Version 1709, verfügbar ist, oder das Remoteserver-Verwaltungstools, das unter Windows Server 2019 verfügbar ist, um einen Linux-Vorlagen Datenträger

```
# Replace "THUMBPRINT" with the thumbprint of your template disk signing certificate in the line below
$certificate = Get-Item Cert:\LocalMachine\My\THUMBPRINT
```

```
Protect-TemplateDisk -Path 'C:\temp\MyLinuxTemplate.vhdx' -TemplateName 'Ubuntu 16.04' -Version 1.0.0.0 -
Certificate $certificate -ProtectedTemplateTargetDiskType PreprocessedLinux
```

Der Vorlagen Datenträger kann jetzt zum Bereitstellen von abgeschirmten Linux-VMs verwendet werden. Wenn Sie System Center Virtual Machine Manager zum Bereitstellen Ihrer VM verwenden, können Sie jetzt die vhd-Datei in die VMM-Bibliothek kopieren.

Möglicherweise möchten Sie auch den volumesignaturkatalog aus der vhd-Datei extrahieren. Diese Datei wird verwendet, um Informationen über das Signaturzertifikat, den Datenträger Namen und die Version für die VM-Besitzer bereitzustellen, die Ihre Vorlage verwenden möchten. Sie müssen diese Datei in den Assistenten für die Schutz Datendatei importieren, um Sie zu autorisieren, den Vorlagen Autor im Besitz des Signatur Zertifikats, um diesen und zukünftige Vorlagen Datenträger zu erstellen.

Führen Sie den folgenden Befehl in PowerShell aus, um den volumesignaturkatalog zu extrahieren:

```
Save-VolumeSignatureCatalog -TemplateDiskPath 'C:\temp\MyLinuxTemplate.vhdx' -VolumeSignatureCatalogPath
'C:\temp\MyLinuxTemplate.vsc'
```

Abgeschirmte VMs: Hosting-Anbieter richtet Windows Azure Pack ein

09.04.2020 • 9 minutes to read • [Edit Online](#)

In diesem Thema wird beschrieben, wie ein hostingdienstanbieter Windows Azure Pack konfigurieren kann, damit Mandanten ihn zum Bereitstellen von abgeschirmten VMS verwenden können. Windows Azure Pack ist ein Webportal, das die Funktionalität von System Center Virtual Machine Manager erweitert, damit Mandanten ihre eigenen VMS über eine einfache Weboberfläche bereitstellen und verwalten können. Windows Azure Pack werden abgeschirmte VMS vollständig unterstützen und die Erstellung und Verwaltung Ihrer geschützten Datendateien für Ihre Mandanten noch einfacher.

Informationen dazu, wie sich dieses Thema in den Gesamtprozess der Bereitstellung von abgeschirmten VMS einfügt, finden Sie unter [Hosten von Dienst Anbietern Konfigurationsschritte für geschützte Hosts und abgeschirmte VMS](#).

Einrichten von Windows Azure Pack

Sie führen die folgenden Aufgaben aus, um Windows Azure Pack in Ihrer Umgebung einzurichten:

1. Vervollständigen Sie die Konfiguration von System Center 2016-Virtual Machine Manager (VMM) für Ihr hostingfabric. Dies umfasst das Einrichten von VM-Vorlagen und eine VM-Cloud, die über Windows Azure Pack verfügbar gemacht wird:

[Szenario: Bereitstellen von überwachten Hosts und abgeschirmten virtuellen Maschinen in VMM](#)

2. Installieren und Konfigurieren von System Center 2016-Service Provider Foundation (SPF). Diese Software ermöglicht Windows Azure Pack die Kommunikation mit Ihren VMM-Servern:

[Bereitstellen von Service Provider Foundation-SPF](#)

3. Installieren Sie Windows Azure Pack, und konfigurieren Sie ihn für die Kommunikation mit SPF:

- [Installieren von Windows Azure Pack](#) (in diesem Thema)
- [Konfigurieren von Windows Azure Pack](#) (in diesem Thema)

4. Erstellen Sie einen oder mehrere hostingpläne in Windows Azure Pack, um Mandanten den Zugriff auf Ihre VM-Clouds zu ermöglichen:

[Erstellen eines Plans in Windows Azure Pack](#) (in diesem Thema)

Installieren von Windows Azure Pack

Installieren und konfigurieren Sie Windows Azure Pack (WAP) auf dem Computer, auf dem Sie das Webportal für Ihre Mandanten hosten möchten. Dieser Computer muss in der Lage sein, den SPF-Server zu erreichen und für Ihre Mandanten erreichbar zu sein.

1. Überprüfen der [WAP-Systemanforderungen](#) und Installieren der [erforderlichen Software](#).
2. Herunterladen und Installieren des [Webplattform-Installers](#). Wenn der Computer nicht mit dem Internet verbunden ist, befolgen Sie die [Anweisungen zur Offline Installation](#).
3. Öffnen Sie den Webplattform-Installer, und suchen Sie nach **Windows Azure Pack: Portal und API Express** auf der Registerkarte **Produkte**. Klicken Sie auf **Hinzufügen**, und **Installieren** Sie dann am unteren Rand des Fensters.

4. Führen Sie die weiteren Schritte der Installation aus. Nachdem die Installation abgeschlossen ist, wird die Konfigurations Website (<https://<wapserver>:30101/>) in Ihrem Webbrowser geöffnet. Geben Sie auf dieser Website Informationen zu Ihrem SQL-Server an, und schließen Sie die Konfiguration von WAP ab.

Hilfe zum Einrichten von Windows Azure Pack finden Sie unter [Installieren einer Express-Bereitstellung Windows Azure Pack](#).

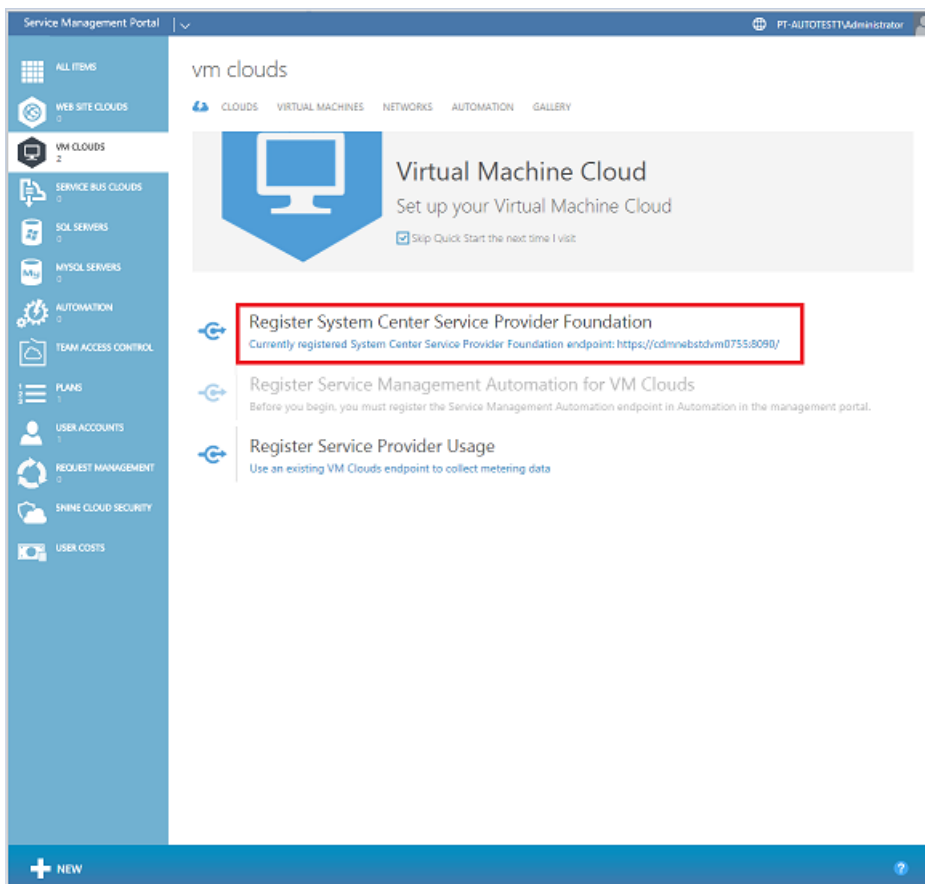
NOTE

Wenn Sie Windows Azure Pack bereits in Ihrer Umgebung ausgeführt haben, können Sie die vorhandene-Installation verwenden. Um mit den neuesten geschützten VM-Features arbeiten zu können, müssen Sie jedoch die Installation auf mindestens Updaterollup 10 aktualisieren.

Konfigurieren von Windows Azure Pack

Bevor Sie Windows Azure Pack verwenden, sollten Sie es bereits installiert und für Ihre Infrastruktur konfiguriert haben.

1. Navigieren Sie zum Windows Azure Pack Admin-Portal unter <https://<wapserver>:30091>, und melden Sie sich dann mit Ihren Administrator Anmelde Informationen an.
2. Klicken Sie im linken Bereich auf **VM-Clouds**.
3. Verbinden Sie Windows Azure Pack mit der Service Provider Foundation Instanz, indem Sie auf **System Center Service Provider Foundation registrieren** klicken. Sie müssen die URL für Service Provider Foundation sowie einen Benutzernamen und ein Kennwort angeben.



4. Nachdem der Vorgang abgeschlossen ist, sollten Sie in der Lage sein, die VM-Clouds in Ihrer VMM-Umgebung einzurichten. Stellen Sie sicher, dass Sie mindestens eine VM-Cloud haben, die abgeschirmte VMS unterstützt, die für WAP verfügbar sind

Erstellen eines Plans in Windows Azure Pack

Damit Mandanten VMs in WAP erstellen können, müssen Sie zuerst einen Hostingplan erstellen, den Mandanten abonnieren können. Pläne definieren die zulässigen VM-Clouds,-Vorlagen,-Netzwerke und-Abrechnungs Entitäten für Ihre Mandanten.

1. Klicken Sie im unteren Bereich des Portals auf **+ neu > Plan > Plan Erstellen**.
2. Wählen Sie im ersten Schritt des Assistenten einen Namen für den Plan aus. Dies ist der Name, den Ihre Mandanten beim Abonnieren sehen.
3. Wählen Sie im zweiten Schritt die Option **VM- Clouds** als einer der Dienste aus, die im Plan angeboten werden sollen.
4. Überspringen Sie den Schritt zum Auswählen von Add-ons für den Plan.
5. Klicken Sie auf **OK** (Häkchen), um den Plan zu erstellen. Obwohl dies den Plan erstellt, befindet er sich noch nicht in einem konfigurierten Zustand.

plans

PLANS ADD-ONS SUBSCRIPTIONS

| NAME | STATUS | STATE | POPULARITY | SUBSCRIPTIONS | PL... | |
|------------------------|-----------|----------------|------------|---------------|-------------|--|
| vNext with Shielded VM | ! Private | Not Configured | 1 | 0 | vNextid8... | |
| 2012R2 Cloud | ! Private | Not Configured | 1 | 0 | RCloud8... | |

6. Um mit der Konfiguration des Plans zu beginnen, klicken Sie auf seinen Namen.
7. Klicken Sie auf der nächsten Seite unter **Plan Dienste** auf **VM- Clouds**. Dadurch wird die Seite geöffnet, auf der Sie Kontingente für diesen Plan konfigurieren können.
8. Wählen Sie unter **Basic** den VMM-Verwaltungs Server und die VM-Cloud aus, die Sie Ihren Mandanten anbieten möchten. Clouds, die abgeschirmte VMS anbieten können, werden mit **(Schutz unterstützt)** neben dem Namen angezeigt.
9. Wählen Sie die Kontingente aus, die Sie in diesem Plan anwenden möchten. (Z. b. Grenzwerte für CPU-Kern und RAM-Auslastung). Vergewissern Sie sich, dass das Kontrollkästchen **Virtual Machines als geschützt zulassen** aktiviert ist.

Service Management Portal | CONTOSO\Administrator

virtual machine clouds

basic

VMM MANAGEMENT SERVER: Contoso9362.contoso.com

VIRTUAL MACHINE CLOUD: ShieldedCloud (shielding supported)

usage limit

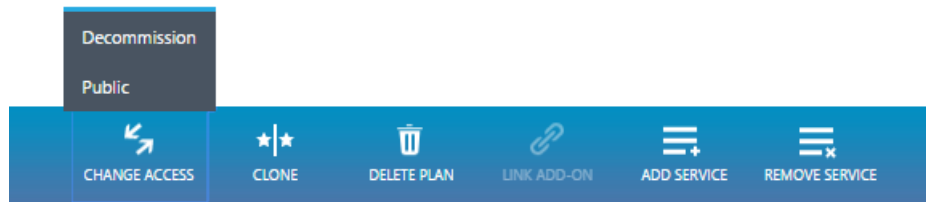
| RESOURCES | AVAILABLE | USE ALL AVAILABLE | USAGE LIMIT |
|------------------|-----------|-------------------------------------|-------------|
| VIRTUAL MACHINES | UNLIMITED | <input checked="" type="checkbox"/> | Unlimited |

☒ Allow Virtual Machines To Be Shielded **PREVIEW**

10. Scrollen Sie nach unten zum Abschnitt **Vorlagen**, und wählen Sie dann eine oder mehrere Vorlagen aus, die

ihren Mandanten angeboten werden sollen. Sie können Mandanten sowohl abgeschirmte als auch unsadierte Vorlagen anbieten, aber es muss eine geschützte Vorlage angeboten werden, um Mandanten eine End-to-End-Zusicherung über die Integrität der VM und ihrer geheimen Schlüssel zu geben.

11. Fügen Sie im Abschnitt " **Netzwerke** " ein oder mehrere Netzwerke für Ihre Mandanten hinzu.
12. Nachdem Sie andere Einstellungen oder Kontingente für den Plan festgelegt haben, klicken Sie unten auf **Speichern** .
13. Klicken Sie oben links auf dem Bildschirm auf den Pfeil, um zur Seite " **Plan** " zurückzukehren.
14. Ändern Sie am unteren Bildschirmrand den Plan von **Privat** in **öffentlich** , damit Mandanten den Plan abonnieren können.



An diesem Punkt ist Windows Azure Pack konfiguriert, und Mandanten können den soeben erstellten Plan abonnieren und abgeschirmte VMS bereitstellen. Weitere Schritte, die Mandanten ausführen müssen, finden Sie unter [abgeschirmte VMs für Mandanten: Bereitstellen einer abgeschirmten VM mithilfe von Windows Azure Pack](#).

Siehe auch

- [Konfigurationsschritte des hostingdiensteanbieters für geschützte Hosts und abgeschirmte VMS](#)
- [Geschütztes Fabric und abgeschirmte VMs](#)

Erstellen einer Antwortdatei für die BS-Spezialisierung

09.04.2020 • 7 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Zur Vorbereitung der Bereitstellung von abgeschirmten VMS müssen Sie möglicherweise eine Antwortdatei für die Betriebssystem Spezialisierung erstellen. Unter Windows wird dies häufig als die Datei "Unattend.xml" bezeichnet. Die Windows PowerShell-Funktion **New-shieldingdataanswerfile** unterstützt Sie dabei. Anschließend können Sie die Antwortdatei verwenden, wenn Sie abgeschirmte VMS mithilfe System Center Virtual Machine Manager (oder einer anderen Fabric Controller) aus einer Vorlage erstellen.

Allgemeine Richtlinien für Dateien für die unbeaufsichtigte Installation für abgeschirmte VMS finden Sie unter [Erstellen einer Antwortdatei](#).

Herunterladen der New-shieldingdataanswerfile-Funktion

Sie können die Funktion **New-shieldingdataanswerfile** aus dem [PowerShell-Katalog](#) abrufen. Wenn Ihr Computer über eine Internet Verbindung verfügt, können Sie ihn mit dem folgenden Befehl aus PowerShell installieren:

```
Install-Module GuardedFabricTools -Repository PSGallery -MinimumVersion 1.0.0
```

Die `unattend.xml` Ausgabe kann zusammen mit zusätzlichen Artefakten in die Schutz Daten gepackt werden, damit Sie zum Erstellen von abgeschirmten VMS aus Vorlagen verwendet werden kann.

In den folgenden Abschnitten wird gezeigt, wie Sie die Funktionsparameter für eine `unattend.xml` Datei mit verschiedenen Optionen verwenden können:

- [Grundlegende Windows-Antwortdatei](#)
- [Windows-Antwortdatei mit Domänen Beitritt](#)
- [Windows-Antwortdatei mit statischen IPv4-Adressen](#)
- [Windows-Antwortdatei mit einem benutzerdefinierten Gebiets Schema](#)
- [Grundlegende Linux-Antwortdatei](#)

Grundlegende Windows-Antwortdatei

Mit den folgenden Befehlen wird eine Windows-Antwortdatei erstellt, die einfach das Kennwort des Administrator Kontos und den Hostnamen festlegt. Die VM-Netzwerkadapter verwenden DHCP zum Abrufen von IP-Adressen, und der virtuelle Computer wird nicht zu einer Active Directory Domäne hinzugefügt. Wenn Sie zur Eingabe von Administrator Anmelde Informationen aufgefordert werden, geben Sie den gewünschten Benutzernamen und das Kennwort an. Verwenden Sie "Administrator" als Benutzername, wenn Sie das integrierte Administrator Konto konfigurieren möchten.

```
$adminCred = Get-Credential -Message "Local administrator account"

New-ShieldingDataAnswerFile -Path '.\ShieldedVMAnswerFile.xml' -AdminCredentials $adminCred
```

Windows-Antwortdatei mit Domänen Beitritt

Mit den folgenden Befehlen wird eine Windows-Antwortdatei erstellt, die den abgeschirmten virtuellen Computer mit einer Active Directory Domäne verbindet. Die VM-Netzwerkadapter verwenden DHCP zum Abrufen von IP-Adressen.

Bei der ersten Eingabeaufforderung werden die Informationen zum lokalen Administrator Konto angefordert. Verwenden Sie "Administrator" als Benutzername, wenn Sie das integrierte Administrator Konto konfigurieren möchten.

Die zweite Eingabeaufforderung fordert Anmelde Informationen an, die über das Recht verfügen, den Computer mit der Active Directory Domäne zu verknüpfen.

Stellen Sie sicher, dass Sie den Wert des Parameters "-Domain Name" in den voll qualifizierten Domänen Namen (FQDN) Ihrer Active Directory Domäne ändern.

```
$adminCred = Get-Credential -Message "Local administrator account"
$domainCred = Get-Credential -Message "Domain join credentials"

New-ShieldingDataAnswerFile -Path '.\ShieldedVMAnswerFile.xml' -AdminCredentials $adminCred -DomainName
'my.contoso.com' -DomainJoinCredentials $domainCred
```

Windows-Antwortdatei mit statischen IPv4-Adressen

Die folgenden Befehle erstellen eine Windows-Antwortdatei, die statische IP-Adressen verwendet, die während der Bereitstellung vom Fabric-Manager bereitgestellt werden, z. b. System Center Virtual Machine Manager

Virtual Machine Manager stellt der statischen IP-Adresse drei Komponenten mithilfe eines IP-Pools bereit: IPv4-Adresse, IPv6-Adresse, Gatewayadresse und DNS-Adresse. Wenn Sie möchten, dass zusätzliche Felder eingeschlossen werden oder eine benutzerdefinierte Netzwerkkonfiguration erforderlich ist, müssen Sie die vom Skript erstellte Antwortdatei manuell bearbeiten.

Die folgenden Screenshots zeigen die IP-Adress Pools, die Sie in Virtual Machine Manager konfigurieren können. Diese Pools sind erforderlich, wenn Sie statische IP-Adressen verwenden möchten.

Derzeit unterstützt die Funktion nur einen DNS-Server. Ihre DNS-Einstellungen würden wie folgt aussehen:

Create Static IP Address Pool Wizard

DNS

Name

Network Site

IP address range

Gateway

DNS

WINS

Summary

Specify one or more DNS servers

DNS server addresses in the order of use:

| DNS Server Address |
|--------------------|
| 10.192.206.99 |

Insert
Delete
Move Up
Move Down

Connection specific DNS suffix:

DNS search suffixes to append (in order):

| DNS Suffix |
|------------|
|------------|

Insert
Delete
Move Up
Move Down

Previous Next Cancel

Im folgenden finden Sie eine Zusammenfassung zum Erstellen des statischen IP-Adress Pools. Kurz gesagt, Sie benötigen nur eine Netzwerk Route, ein Gateway und einen DNS-Server, und Sie müssen Ihre IP-Adresse angeben.

Create Static IP Address Pool Wizard

Summary

Name

Network Site

IP address range

Gateway

DNS

WINS

Summary

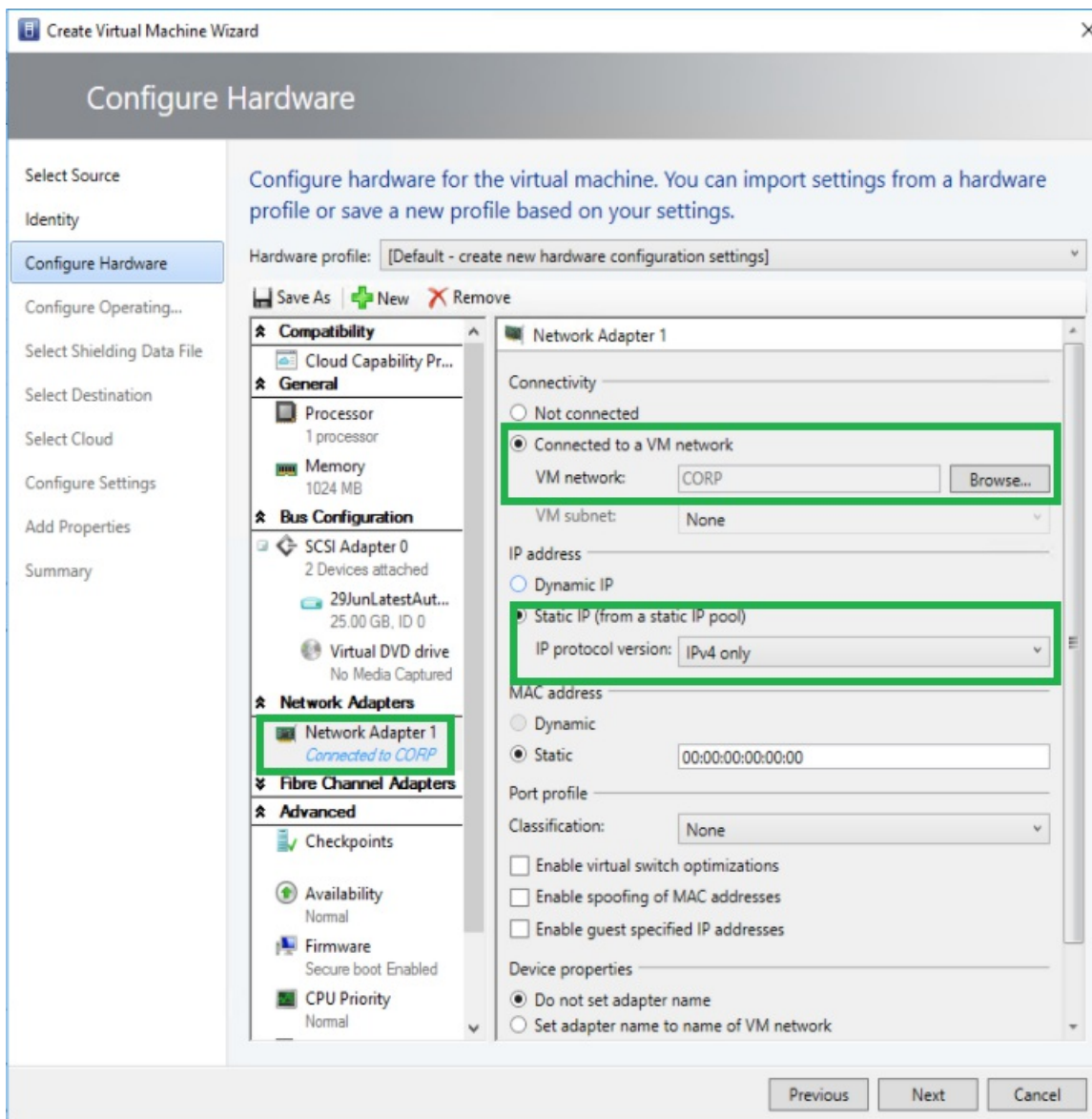
Confirm the settings

View Script

| | |
|---------------------------------|-----------------------------|
| Name: | IpPool |
| Description: | |
| IP subnet: | 10.184.110.0/23 |
| IP address range: | 10.184.110.1-10.184.111.254 |
| Connection specific DNS suffix: | |
| Network routes: | 1 Network routes |
| Gateways: | 1 Gateways |
| DNS servers: | 1 DNS servers |
| WINS servers: | 0 WINS servers |

Previous Finish Cancel

Sie müssen Ihren Netzwerkkadpter für den virtuellen Computer konfigurieren. Der folgende Screenshot zeigt, wo Sie diese Konfiguration festlegen können und wie Sie Sie in statische IP-Adressen wechseln.



Anschließend können Sie den `-StaticIPPool`-Parameter verwenden, um die statischen IP-Elemente in die Antwortdatei einzuschließen. Die Parameter `@IPAddr-1@`, `@NextHop-1-1@` und `@DNSAddr-1-1@` in der Antwortdatei werden dann durch die tatsächlichen Werte ersetzt, die Sie zum Zeitpunkt der Bereitstellung in Virtual Machine Manager angegeben haben.

```
$adminCred = Get-Credential -Message "Local administrator account"

New-ShieldingDataAnswerFile -Path '.\ShieldedVMAnswerFile.xml' -AdminCredentials $adminCred -StaticIPPool
IPv4Address
```

Windows-Antwortdatei mit einem benutzerdefinierten Gebiets Schema

Mit den folgenden Befehlen wird eine Windows-Antwortdatei mit einem benutzerdefinierten Gebiets Schema erstellt.

Wenn Sie zur Eingabe von Administrator Anmelde Informationen aufgefordert werden, geben Sie den gewünschten Benutzernamen und das Kennwort an. Verwenden Sie "Administrator" als Benutzername, wenn Sie das integrierte Administrator Konto konfigurieren möchten.

```
$adminCred = Get-Credential -Message "Local administrator account"
$domainCred = Get-Credential -Message "Domain join credentials"

New-ShieldingDataAnswerFile -Path '.\ShieldedVMAnswerFile.xml' -AdminCredentials $adminCred -Locale es-ES
```

Grundlegende Linux-Antwortdatei

Ab Windows Server, Version 1709, können Sie bestimmte Linux-Gast Betriebssysteme auf abgeschirmten VMS ausführen. Wenn Sie den System Center Virtual Machine Manager Linux-Agent verwenden, um diese VMS zu spezialisieren, kann das Cmdlet New-shieldingdataanswerfile kompatible Antwort Dateien für das Cmdlet erstellen.

In einer Linux-Antwortdatei enthalten Sie in der Regel das Stamm Kennwort, den Stamm-SSH-Schlüssel und optional Informationen zum statischen IP-Pool. Ersetzen Sie den Pfad zur öffentlichen Hälfte Ihres SSH-Schlüssels, bevor Sie das folgende Skript ausführen.

```
$rootPassword = Read-Host -Prompt "Root password" -AsSecureString

New-ShieldingDataAnswerFile -Path '.\ShieldedVMAnswerFile.xml' -RootPassword $rootPassword -RootSshKey
'~\.ssh\id_rsa.pub'
```

Siehe auch

- [Bereitstellen von abgeschirmten VMs](#)
- [Geschütztes Fabric und abgeschirmte VMs](#)

Abgeschirmte VMs für Mandanten: Erstellen von Schutz Daten zum Definieren einer abgeschirmten VM

09.04.2020 • 29 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Eine geschützte Datendatei (auch als Bereitstellungsdatendatei oder PDK-Datei bezeichnet) ist eine verschlüsselte Datei, die ein Mandant oder VM-Besitzer erstellt, um wichtige VM-Konfigurationsinformationen, z.B. Administratorkennwort, RDP und andere identitätsbezogene Zertifikate, Domänenbeitritts-Anmeldeinformationen usw. zu schützen. Dieses Thema enthält Informationen zum Erstellen einer Schutz Datendatei. Bevor Sie die Datei erstellen können, müssen Sie entweder einen Vorlagen Datenträger von Ihrem hostingdienstanbieter abrufen oder einen Vorlagen Datenträger erstellen, wie unter [abgeschirmte VMs für Mandanten: Erstellen eines Vorlagen Datenträgers](#) (optional) beschrieben.

Eine Liste und ein Diagramm mit dem Inhalt einer Schutz Datendatei finden [Sie unter Was sind geschützte Daten? und warum ist es erforderlich?](#).

IMPORTANT

Die Schritte in diesem Abschnitt sollten auf einem separaten, vertrauenswürdigen Computer außerhalb des geschützten Fabrics ausgeführt werden. Normalerweise erstellt der VM-Besitzer (Mandant) die geschützten Daten für Ihre VMS, nicht die Fabric-Administratoren.

Führen Sie die folgenden Schritte aus, um eine Schutz Datendatei zu erstellen:

- [Abrufen eines Zertifikats für Remotedesktopverbindung](#)
- [Erstellen einer Antwortdatei](#)
- [Get the Volume Signature Catalog file](#)
- [Vertrauenswürdige Fabrics auswählen](#)

Anschließend können Sie die geschützte Datendatei erstellen:

- [Erstellen einer Schutz Datendatei und Hinzufügen von Betreuern](#)

Optionale Abrufen eines Zertifikats für Remotedesktopverbindung

Da Mandanten nur über Remotedesktopverbindung oder andere Remote Verwaltungs Tools eine Verbindung mit ihren abgeschirmten VMS herstellen können, ist es wichtig sicherzustellen, dass Mandanten sicherstellen können, dass Sie eine Verbindung mit dem richtigen Endpunkt herstellen (d. h. es ist kein "man in der Mitte"). die Verbindung wird abgefangen).

Eine Möglichkeit, um zu überprüfen, ob Sie eine Verbindung mit dem vorgesehenen Server herstellen, ist die Installation und Konfiguration eines Zertifikats, das Remotedesktopdienste beim Initiieren einer Verbindung vorhanden ist. Der Client Computer, der eine Verbindung mit dem Server herstellt, prüft, ob das Zertifikat vertrauenswürdig ist, und zeigt eine Warnung an. Im Allgemeinen werden RDP-Zertifikate von der PKI des Mandanten ausgegeben, um sicherzustellen, dass der Verbindungs Client dem Zertifikat vertraut. Weitere Informationen zur [Verwendung von Zertifikaten in Remotedesktopdienste finden Sie](#) im TechNet.

Beachten Sie Folgendes, um Sie bei der Entscheidung zu unterstützen, ob Sie ein benutzerdefiniertes RDP-Zertifikat erhalten müssen:

- Wenn Sie nur abgeschirmte VMs in einer Lab-Umgebung testen, benötigen Sie **kein** benutzerdefiniertes RDP-Zertifikat.
- Wenn Ihr virtueller Computer für den Beitritt zu einer Active Directory Domäne konfiguriert ist, wird in der Regel von der Zertifizierungsstelle Ihres Unternehmens automatisch ein Computer Zertifikat ausgestellt und zum Identifizieren des Computers bei RDP-Verbindungen verwendet. Sie benötigen **kein** benutzerdefiniertes RDP-Zertifikat.
- Wenn Ihr virtueller Computer keiner Domäne beigetreten ist, Sie jedoch sicherstellen möchten, dass Sie eine Verbindung mit dem richtigen Computer herstellen, wenn Sie Remotedesktop verwenden, sollten Sie die Verwendung von benutzerdefinierten RDP-Zertifikaten in **Erwägung gezogen** .

TIP

Wenn Sie ein RDP-Zertifikat auswählen, das in die geschützte Datendatei aufgenommen werden soll, achten Sie darauf, ein Platzhalter Zertifikat zu verwenden. Eine geschützte Datendatei kann verwendet werden, um eine unbegrenzte Anzahl von VMS zu erstellen. Da jeder virtuelle Computer das gleiche Zertifikat verwendet, wird durch ein Platzhalter Zertifikat sichergestellt, dass das Zertifikat unabhängig vom Hostnamen des virtuellen Computers gültig ist.

Erstellen einer Antwortdatei

Da der signierte Vorlagen Datenträger in VMM generalisiert ist, müssen Mandanten eine Antwortdatei bereitstellen, um Ihre abgeschirmten VMs während des Bereitstellungs Prozesses zu spezialisieren. Die Antwortdatei (häufig als Datei für die unbeaufsichtigte Installation bezeichnet) kann den virtuellen Computer für die beabsichtigte Rolle konfigurieren, d. h., er kann Windows-Features installieren, das im vorherigen Schritt erstellte RDP-Zertifikat registrieren und andere benutzerdefinierte Aktionen ausführen. Außerdem werden die erforderlichen Informationen für das Windows-Setup bereitgestellt, einschließlich des Standard Kennworts für den Administrator und Product Key.

Weitere Informationen zum Abrufen und Verwenden der **New-shieldingdataanswer File**- Funktion, um eine Antwortdatei (Unattend. XML-Datei) zum Erstellen von abgeschirmten VMS zu generieren, finden Sie unter [Generieren einer Antwortdatei mithilfe der New-shieldingdataantwortungsdateifunktion](#). Mithilfe der-Funktion können Sie eine Antwortdatei, die die folgenden Optionen widerspiegelt, einfacher generieren:

- Soll der virtuelle Computer am Ende des Initialisierungs Prozesses in eine Domäne aufgenommen werden?
- Verwenden Sie eine Volumenlizenz oder eine bestimmte Product Key pro VM?
- Verwenden Sie DHCP oder eine statische IP-Adresse?
- Verwenden Sie ein benutzerdefiniertes Remotedesktopprotokoll Zertifikat (RDP), das verwendet wird, um nachzuweisen, dass der virtuelle Computer zu Ihrer Organisation gehört?
- Möchten Sie ein Skript am Ende der Initialisierung ausführen?

Antwort Dateien, die in geschützten Datendateien verwendet werden, werden auf allen virtuellen Computern verwendet, die mit dieser Schutz Datendatei erstellt werden. Daher sollten Sie sicherstellen, dass Sie keine VM-spezifischen Informationen in der Antwortdatei hart codieren. VMM unterstützt einige Ersatz Zeichenfolgen (siehe Tabelle unten) in der Datei für die unbeaufsichtigte Installation, um Spezialisierungs Werte zu verarbeiten, die sich möglicherweise von VM zu VM ändern Sie müssen diese nicht verwenden. Wenn Sie jedoch vorhanden sind, werden diese von VMM genutzt.

Beachten Sie beim Erstellen einer Datei "Unattend.xml" für abgeschirmte VMS die folgenden Einschränkungen:

- Wenn Sie VMM zum Verwalten Ihres Rechenzentrums verwenden, muss die Datei für die unbeaufsichtigte Installation nach der Konfiguration des virtuellen Computers ausgeschaltet werden. Auf diese Weise kann VMM wissen, wann dem Mandanten berichtet werden soll, dass die VM bereitgestellt wurde und

einsatzbereit ist. Der virtuelle Computer wird von VMM automatisch wieder eingeschaltet, sobald erkannt wird, dass er während der Bereitstellung deaktiviert wurde.

- Stellen Sie sicher, dass Sie RDP und die entsprechende Firewallregel aktivieren, damit Sie nach der Konfiguration auf den virtuellen Computer zugreifen können. Sie können die VMM-Konsole nicht verwenden, um auf abgeschirmte VMS zuzugreifen, sodass Sie RDP benötigen, um eine Verbindung mit Ihrem virtuellen Computer herzustellen. Wenn Sie Ihre Systeme mit Windows PowerShell-Remoting verwalten möchten, müssen Sie auch sicherstellen, dass WinRM ebenfalls aktiviert ist.
- Die einzigen Ersetzungs Zeichenfolgen, die von Dateien für die unbeaufsichtigte Installation geschützter VMS unterstützt werden,

| ERSETZBARES ELEMENT | ERSATZ ZEICHENFOLGE |
|---------------------|---------------------|
| Computername | @ComputerName@ |
| TimeZone | @TimeZone@ |
| ProduktKey | @ProductKey@ |
| IPAddr4-1 | @IP4Addr-1@ |
| IPAddr6-1 | @IP6Addr-1@ |
| MACADDR-1 | @MACAddr-1@ |
| Präfix-1-1 | @Prefix-1-1@ |
| NextHop-1-1 | @NextHop-1-1@ |
| Präfix-1-2 | @Prefix-1-2@ |
| NextHop-1-2 | @NextHop-1-2@ |

Wenn Sie über mehr als eine NIC verfügen, können Sie mehrere Ersatz Zeichenfolgen für die IP-Konfiguration hinzufügen, indem Sie die erste Ziffer erhöhen. Wenn Sie z. B. die IPv4-Adresse, das Subnetz und das Gateway für zwei NICs festlegen möchten, verwenden Sie die folgenden Ersetzungs Zeichenfolgen:

| ERSATZ ZEICHENFOLGE | BEISPIEL ERSETZUNG |
|---------------------|--------------------|
| @IP4Addr-1@ | 192.168.1.10/24 |
| @MACAddr-1@ | Ethernet |
| @Prefix-1-1@ | 24 |
| @NextHop-1-1@ | 192.168.1.254 |
| @IP4Addr-2@ | 10.0.20.30/24 |
| @MACAddr-2@ | Ethernet 2 |

| ERSATZ ZEICHENFOLGE | BEISPIEL ERSETZUNG |
|---------------------|--------------------|
| @Prefix-2-1@ | 24 |
| @NextHop-2-1@ | 10.0.20.1 |

Bei der Verwendung von Ersetzungs Zeichenfolgen müssen Sie sicherstellen, dass die Zeichen folgen während des VM-Bereitstellungs Prozesses aufgefüllt werden. Wenn eine Zeichenfolge wie @ProductKey@ zum Zeitpunkt der Bereitstellung nicht angegeben wird, während der <ProductKey-> Knoten in der Datei für die unbeaufsichtigte Installation leer bleibt, schlägt der Spezialisierungsprozess fehl, und Sie können keine Verbindung mit dem virtuellen Computer herstellen.

Beachten Sie außerdem, dass die netzwerkbezogenen Ersetzungs Zeichenfolgen für das Ende der Tabelle nur verwendet werden, wenn Sie statische VMM-IP-Adress Pools nutzen. Ihr hostingdienstanbieter sollte Ihnen mitteilen können, ob diese Ersetzungs Zeichenfolgen erforderlich sind. Weitere Informationen zu statischen IP-Adressen in VMM-Vorlagen finden Sie in der folgenden Dokumentation in der VMM-Dokumentation:

- [Richtlinien für IP-Adress Pools](#)
- [Einrichten von statischen IP-Adress Pools im VMM-Fabric](#)

Schließlich ist es wichtig zu beachten, dass bei der Bereitstellung der abgeschirmten VM nur das Betriebssystem Laufwerk verschlüsselt wird. Wenn Sie einen abgeschirmten virtuellen Computer mit einem oder mehreren Daten Laufwerken bereitstellen, wird dringend empfohlen, dass Sie einen Unattend-Befehl oder Gruppenrichtlinie Einstellung in der Mandanten Domäne hinzufügen, um die Daten Laufwerke automatisch zu verschlüsseln.

Get the Volume Signature Catalog file

Geschützte Datendateien enthalten auch Informationen zu den Vorlagen Datenträgern, denen ein Mandant vertraut. Mandanten erhalten die Datenträger Signaturen von vertrauenswürdigen Vorlagen Datenträgern in Form einer volumesignatur-Katalog Datei (VSC). Diese Signaturen werden dann überprüft, wenn ein neuer virtueller Computer bereitgestellt wird. Wenn keine der Signaturen in der Schutz Datendatei mit dem Vorlagen Datenträger, der mit dem virtuellen Computer bereitgestellt werden soll, identisch ist (d. h., er wurde geändert oder mit einem anderen, potenziell bösartigen Datenträger ausgetauscht), schlägt der Bereitstellungs Vorgang fehl.

IMPORTANT

Während der VSC sicherstellt, dass ein Datenträger nicht manipuliert wurde, ist es weiterhin wichtig, dass der Mandant den Datenträger zunächst als vertrauenswürdig einstuft. Wenn Sie der Mandant sind und der Vorlagen Datenträger von Ihrem Host bereitgestellt wird, stellen Sie einen virtuellen Testcomputer mit diesem Vorlagen Datenträger bereit, und führen Sie eigene Tools (Antivirus, Sicherheitsrisiko Scanner usw.) aus, um zu überprüfen, ob der Datenträger tatsächlich in einem vertrauenswürdig Zustand ist.

Es gibt zwei Möglichkeiten, den VSC eines Vorlagen Datenträgers abzurufen:

1. Der Host (oder Mandant), wenn der Mandant auf VMM zugreifen kann, verwendet die VMM-PowerShell-Cmdlets zum Speichern des VSC und übergibt ihn an den Mandanten. Dies kann auf einem beliebigen Computer ausgeführt werden, auf dem die VMM-Konsole installiert und konfiguriert ist, um die VMM-Umgebung des hostingfabrics zu verwalten. Die PowerShell-Cmdlets zum Speichern des VSC lauten wie folgt:

```
$disk = Get-SCVirtualHardDisk -Name "templateDisk.vhdx"

$jsc = Get-SCVolumeSignatureCatalog -VirtualHardDisk $disk

$jsc.WriteToFile(".\templateDisk.vsc")
```

2. Der Mandant hat Zugriff auf die Vorlagen Datenträger-Datei. Dies kann der Fall sein, wenn der Mandant einen Vorlagen Datenträger erstellt, der auf einen hostingdienstanbieter hochgeladen werden soll, oder wenn der Mandant den Vorlagen Datenträger des gehosteten In diesem Fall würde der Mandant das folgende Cmdlet ausführen (installiert mit dem Feature "abgeschirmte VM-Tools", das Teil Remoteserver-Verwaltungstools ist), ohne dass VMM in der Abbildung dargestellt wird:

```
Save-VolumeSignatureCatalog -TemplateDiskPath templateDisk.vhdx -VolumeSignatureCatalogPath  
templateDisk.vsc
```

Vertrauenswürdige Fabrics auswählen

Die letzte Komponente in der Schutz Datendatei bezieht sich auf den Besitzer und die Wächter eines virtuellen Computers. Wächter werden verwendet, um den Besitzer einer abgeschirmten VM und die geschützten Fabrics anzugeben, auf denen Sie zur Laufzeit autorisiert ist.

Zum Autorisieren eines hostinganbieters zum Ausführen einer abgeschirmten VM müssen Sie die Überwachungs Metadaten vom Host-Überwachungsdienst des hostingdienstanbieters abrufen. Häufig stellt der hostingdienstanbieter diese Metadaten über die Verwaltungs Tools bereit. In einem Unternehmens Szenario haben Sie möglicherweise direkten Zugriff, um die Metadaten selbst abzurufen.

Sie oder Ihr hostingdienstanbieter können die Überwachungs Metadaten von HGS abrufen, indem Sie eine der folgenden Aktionen ausführen:

- Rufen Sie die Überwachungs Metadaten direkt von HGS ab, indem Sie den folgenden Windows PowerShell-Befehl ausführen, oder navigieren Sie zur Website, und speichern Sie die angezeigte XML-Datei:

```
Invoke-WebRequest 'http://hgs.bastion.local/KeyProtection/service/metadata/2014-07/metadata.xml' -  
OutFile .\RelecloudGuardian.xml
```

- Abrufen der Überwachungs Metadaten von VMM mithilfe der VMM-PowerShell-Cmdlets:

```
$relecloudmetadata = Get-SCGuardianConfiguration  
$relecloudmetadata.InnerXml | Out-File .\RelecloudGuardian.xml -Encoding UTF8
```

Rufen Sie die Überwachungs Metadateien für jedes geschützte Fabric ab, für das Sie Ihre abgeschirmten VMS autorisieren möchten, bevor Sie fortfahren.

Erstellen einer Schutz Datendatei und Hinzufügen von Betreuern mithilfe des Assistenten zum Schützen von Datendateien

Führen Sie den Assistenten für die Schutz Datendatei aus, um eine Datei mit geschützten Daten (PDK) zu erstellen. Hier fügen Sie das RDP-Zertifikat, die Datei für die unbeaufsichtigte Installation, volumesignaturkataloge, den Besitzer Wächter und die heruntergeladenen Überwachungs Metadaten hinzu, die im vorherigen Schritt abgerufen wurden.

1. Installieren Sie mithilfe Server-Manager oder des folgenden Windows PowerShell-Befehls **Remoteserver-**

Install-WindowsFeature RSAT-Shielded-VM-Tools

- Öffnen Sie den Assistenten zum Schützen von Datendateien über den Abschnitt "Administrator Tools" im Startmenü, oder führen Sie die folgende ausführbare Datei "**C:\Windows\System32\shieldingdatafilewizard.exe**" aus.
- Verwenden Sie auf der ersten Seite das zweite Feld für die Auswahl von Dateien, um einen Speicherort und Dateinamen für die geschützte Datendatei auszuwählen. Normalerweise würden Sie eine geschützte Datendatei nach der Entität benennen, die virtuelle Computer besitzt, die mit den geschützten Daten (z. B. HR, IT, Finance) erstellt wurden, und die von ihr ausgestellte workloadrolle (z. B. Dateiserver, Webserver oder etwas anderes, das von der Datei für die unbeaufsichtigte Installation konfiguriert wurde). Lassen Sie das Optionsfeld auf **geschützte Daten für geschützte Vorlagen** fest.

NOTE

Im Assistenten für Schutz Datendateien werden Ihnen die folgenden beiden Optionen angezeigt:

- **Geschützte Daten für geschützte Vorlagen**
- **Schutz von Daten für vorhandene VMS und nicht abgeschirmte Vorlagen**

Die erste Option wird verwendet, wenn neue abgeschirmte VMS aus abgeschirmten Vorlagen erstellt werden. Die zweite Option ermöglicht es Ihnen, geschützte Daten zu erstellen, die nur beim Umrechnen vorhandener virtueller Computer oder beim Erstellen von abgeschirmten VMS aus nicht abgeschirmten Vorlagen verwendet werden können.

The screenshot shows the 'Shielding Data File Wizard' window, specifically the 'File and Policy Selection' step. The window has a title bar with standard Windows controls. On the left is a navigation pane with the following items: 'File and Policy Selection' (highlighted), 'Owner and Guardians', 'Volume ID Qualifiers', 'Specialization Values', 'Review Settings', 'Shielding Data File Gener...', and 'Summary'. The main area contains two radio button options: 'Import and edit an existing shielding data file' and 'Create a new shielding data file' (which is selected). Below the first option is a text field for 'Shielding data file:' with a 'Browse' button. Below the second option is a text field containing 'C:\temp\Marketing-HBI.pdk' with a 'Browse' button. Underneath are two radio button options for the policy: 'Shielding data for Shielded templates' (selected) and 'Shielding data for existing VMs and non-Shielded templates'. Below these is a section titled 'Virtual Machines that use this shielding data file will become:' with two radio button options: 'Shielded' (selected) and 'Encryption Supported'. The 'Shielded' option has a description: 'All security settings are enabled, including disk encryption, and cannot be reconfigured by Hyper-V administrators. Console access to the Virtual Machine is not permitted.' The 'Encryption Supported' option has a description: 'Supports disk encryption and permits Hyper-V administrators to configure other security settings as needed.' At the bottom of the window are four buttons: '< Previous', 'Next >', 'Generate', and 'Cancel'.

Außerdem müssen Sie auswählen, ob VMS, die mit dieser Schutz Datendatei erstellt wurden, im Modus "Verschlüsselung unterstützt" wirklich geschützt oder konfiguriert werden. Weitere Informationen zu diesen beiden Optionen finden Sie unter [Was sind die Typen von virtuellen Maschinen, die von einem geschützten Fabric ausgeführt werden können?](#).

IMPORTANT

Achten Sie sorgfältig auf den nächsten Schritt, da der Besitzer der abgeschirmten VMS und die Fabrics definiert werden, auf denen Ihre abgeschirmten VMS autorisiert sind.

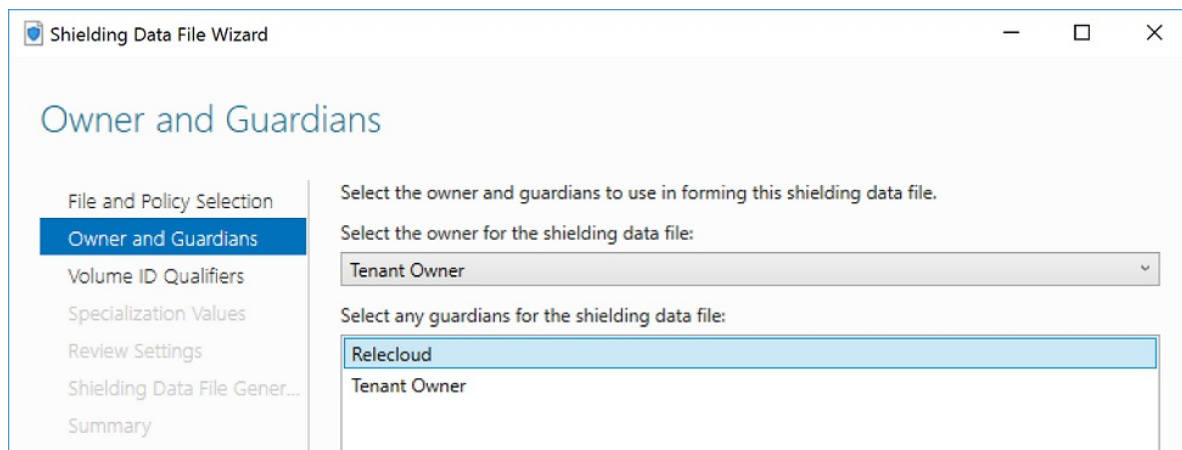
Der Besitz des **Besitzer-Schützers** ist erforderlich, um eine vorhandene abgeschirmte VM später von **abgeschirmt** in **Verschlüsselung unterstützt** oder umgekehrt zu ändern.

4. Ihr Ziel in diesem Schritt besteht darin, das zwei fache zu erreichen:

- Erstellen oder Auswählen eines Besitzer-Schützers, der Sie als VM-Besitzer darstellt
- Importieren Sie den Wächter, den Sie im vorherigen Schritt aus dem (oder Ihrem eigenen) hostüberwachungs Dienst des hostinganbieters heruntergeladen haben.

Um einen vorhandenen Besitzer Wächter festzulegen, wählen Sie im Dropdown Menü den entsprechenden Wächter aus. Nur Wächter, die auf dem lokalen Computer mit den privaten Schlüsseln installiert sind, werden in dieser Liste angezeigt. Sie können auch einen eigenen Besitzer Wächter erstellen, indem Sie in der unteren rechten Ecke **lokale Wächter verwalten** auswählen und auf **Erstellen** klicken, um den Assistenten abzuschließen.

Als nächstes importieren wir die zuvor heruntergeladenen Wächter-Metadaten auf der Seite **Besitzer und Wächter** . Wählen Sie in der unteren rechten Ecke **lokale Wächter verwalten** aus. Verwenden Sie die **Import** Funktion, um die Datei mit den Überwachungs Metadaten zu importieren. Klicken Sie auf **OK** , nachdem Sie alle erforderlichen Wächter importiert oder eingefügt haben. Als bewährte Vorgehensweise können Sie die Wächter nach dem hostingdienstanbieter oder dem Unternehmens Rechenzentrum benennen. Wählen Sie abschließend alle Wächter aus, die die Daten Center darstellen, in denen Ihre abgeschirmte VM ausgeführt werden soll. Sie müssen den Besitzer Wächter nicht erneut auswählen. Klicken Sie **anschließend auf weiter** .



5. Klicken Sie auf der Seite "Volumen-ID-Qualifizierer" auf **Hinzufügen** , um einen signierten Vorlagen Datenträger in der Wenn Sie im Dialogfeld einen VSC auswählen, werden Informationen über den Namen, die Version und das Zertifikat des Datenträgers angezeigt, der zum Signieren verwendet wurde. Wiederholen Sie diesen Vorgang für jeden zu autorisierende Vorlagen Datenträger.
6. Klicken Sie auf der Seite " **Spezialisierungs Werte** " auf **Durchsuchen** , um die Datei "Unattend.xml" auszuwählen, die für die Spezialisierung ihrer VMS verwendet wird.

Verwenden Sie die Schaltfläche **Hinzufügen** am unteren Rand, um dem PDK weitere Dateien hinzuzufügen, die während des Spezialisierungs Vorgangs benötigt werden. Wenn die Datei für die unbeaufsichtigte Installation z. b. ein RDP-Zertifikat auf dem virtuellen Computer installiert (wie unter [Generieren einer Antwortdatei mithilfe der New-shieldingdatabeantwortungsfile-Funktion](#) beschrieben), sollten Sie hier die PFX-Datei des RDP-Zertifikats und das Skript "rdpcertifpteconfig. ps1" hinzufügen. Beachten Sie, dass alle Dateien, die Sie hier angeben, automatisch nach C:\Temp\ auf dem virtuellen

Computer kopiert werden, der erstellt wird. Die Datei für die unbeaufsichtigte Installation sollte erwarten, dass sich die Dateien in diesem Ordner befinden, wenn Sie über den Pfad referenziert werden.

7. Überprüfen Sie Ihre Auswahl auf der nächsten Seite, und klicken Sie dann auf **generieren**.

8. Schließen Sie den Assistenten, nachdem er abgeschlossen wurde.

Erstellen einer Schutz Datendatei und Hinzufügen von Betreuern mithilfe von PowerShell

Als Alternative zum Assistenten zum Schützen von Datendateien können Sie [New-shieldingdatafile](#) ausführen, um eine geschützte Datendatei zu erstellen.

Alle Schutz Datendateien müssen mit den richtigen Besitzer- und Überwachungs Zertifikaten konfiguriert werden, damit Ihre abgeschirmten VMS auf einem geschützten Fabric ausgeführt werden können. Durch Ausführen von [Get-hgsguardian](#) können Sie überprüfen, ob eine lokale Installation vorhanden ist. Besitzer Wächter verfügen über private Schlüssel, während Wächter für Ihr Rechenzentrum dies in der Regel nicht tun.

Wenn Sie einen Owner-Wächter erstellen müssen, führen Sie den folgenden Befehl aus:

```
New-HgsGuardian -Name "Owner" -GenerateCertificates
```

Mit diesem Befehl werden ein paar Signierungs- und Verschlüsselungs Zertifikate im Zertifikat Speicher des lokalen Computers unter dem Ordner "geschützte VM local-Zertifikate" erstellt. Sie benötigen die Besitzer Zertifikate und die zugehörigen privaten Schlüssel, um einen virtuellen Computer zu bereinigen. Stellen Sie also sicher, dass diese Zertifikate gesichert und vor Diebstahl geschützt werden. Ein Angreifer, der Zugriff auf die Besitzer Zertifikate hat, kann ihn verwenden, um den abgeschirmten virtuellen Computer zu starten oder seine Sicherheitskonfiguration zu ändern.

Wenn Sie Überwachungsinformationen aus einem geschützten Fabric importieren müssen, auf dem Sie den virtuellen Computer (Ihr primäres Daten Center, Sicherungs Datacenter usw.) ausführen möchten, führen Sie den folgenden Befehl für jede [Metadatendatei aus, die von ihren geschützten Fabrics abgerufen wird](#).

```
Import-HgsGuardian -Name 'EAST-US Datacenter' -Path '.\EastUSGuardian.xml'
```

TIP

Wenn Sie selbst signierte Zertifikate verwendet haben oder die Zertifikate, die bei HGS registriert sind, abgelaufen sind, müssen Sie möglicherweise die `-AllowUntrustedRoot` -und/oder `-AllowExpired` -Flags mit dem Befehl "Import-hgsguardian" verwenden, um die Sicherheitsüberprüfungen zu umgehen.

Sie müssen auch [einen volumesignaturkatalog](#) für jeden Vorlagen Datenträger abrufen, den Sie mit dieser Schutz Datendatei verwenden möchten, und eine [Antwortdatei](#) für die Schutz Daten, damit das Betriebssystem seine Spezialisierungs Aufgaben automatisch ausführen kann. Entscheiden Sie abschließend, ob Sie möchten, dass Ihr virtueller Computer vollständig abgeschirmt oder nur vtpm aktiviert ist. Verwenden Sie `-Policy Shielded` für eine vollständig abgeschirmte VM oder `-Policy EncryptionSupported` für eine vtpm-aktivierte VM, die einfache Konsolen Verbindungen und PowerShell Direct zulässt.

Nachdem Sie alles vorbereitet haben, führen Sie den folgenden Befehl aus, um die geschützte Datendatei zu erstellen:

```
$viq = New-VolumeIDQualifier -VolumeSignatureCatalogFilePath 'C:\temp\marketing-ws2016.vsc' -VersionRule  
Equals  
New-ShieldingDataFile -ShieldingDataFilePath "C:\temp\Marketing-LBI.pdk" -Policy EncryptionSupported -Owner  
'Owner' -Guardian 'EAST-US Datacenter' -VolumeIDQualifier $viq -AnswerFile 'C:\temp\marketing-ws2016-  
answerfile.xml'
```

TIP

Wenn Sie ein benutzerdefiniertes RDP-Zertifikat, SSH-Schlüssel oder andere Dateien verwenden, die in die geschützte Datendatei eingeschlossen werden müssen, verwenden Sie den `-OtherFile` -Parameter, um diese einzuschließen. Sie können eine durch Trennzeichen getrennte Liste mit Dateipfaden angeben, z. b.

```
-OtherFile "C:\source\myRDPcert.pfx", "C:\source\RDPCertificateConfig.ps1"
```

Im obigen Befehl kann der Wächter mit dem Namen "Owner" (abgerufen von Get-hgsguardian) die Sicherheitskonfiguration des virtuellen Computers in Zukunft ändern, während "East-US Datacenter" den virtuellen Computer ausführen, aber seine Einstellungen nicht ändern kann. Wenn Sie über mehr als einen Wächter verfügen, trennen Sie die Namen der Wächter durch Kommas wie

`'EAST-US Datacenter', 'EMEA Datacenter'`. Der Lautstärke-ID-Qualifizierer gibt an, ob Sie nur der exakten Version (gleich) des Vorlagen Datenträgers oder zukünftigen Versionen (greaterthanorgleich) Vertrauen. Der Datenträger Name und das Signaturzertifikat müssen exakt mit dem Versionsvergleich übereinstimmen, der zum Zeitpunkt der Bereitstellung berücksichtigt wird. Sie können mehr als einem Vorlagen Datenträger Vertrauen, indem Sie eine durch Trennzeichen getrennte Liste mit Volumen-ID-Qualifizierern für den `-VolumeIDQualifier` -Parameter. Wenn Sie weitere Dateien haben, die die Antwortdatei mit dem virtuellen Computer begleiten müssen, verwenden Sie den `-OtherFile` -Parameter, und geben Sie eine durch Trennzeichen getrennte Liste mit Dateipfaden an.

Weitere Informationen zu weiteren Möglichkeiten zum Konfigurieren ihrer geschützten Datendatei finden Sie in der Cmdlet-Dokumentation für [New-shieldingdatafile](#) und [New-volumeidqualifizierer](#).

Siehe auch

- [Bereitstellen von abgeschirmten VMs](#)
- [Geschütztes Fabric und abgeschirmte VMs](#)

Erstellen einer abgeschirmten VM mithilfe von PowerShell

09.04.2020 • 7 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

In der Produktionsumgebung verwenden Sie in der Regel einen Fabric-Manager (z. B. VMM), um abgeschirmte VMS bereitzustellen. Die unten dargestellten Schritte ermöglichen Ihnen jedoch, das gesamte Szenario ohne Fabric-Manager bereitzustellen und zu überprüfen.

Kurz gesagt, erstellen Sie einen Vorlagen Datenträger, eine geschützte Datendatei, eine Antwortdatei für die unbeaufsichtigte Installation und andere Sicherheits Artefakte auf einem beliebigen Computer. Kopieren Sie diese Dateien dann auf einen überwachten Host, und stellen Sie die abgeschirmte VM bereit.

Erstellen einer signierten Vorlagen Festplatte

Zum Erstellen einer neuen abgeschirmten VM benötigen Sie zunächst einen abgeschirmten VM-Vorlagen Datenträger, der mit dem zugehörigen Betriebssystem Volume (bzw. Start- und Stamm Partitionen unter Linux) vorverschlüsselt ist. Befolgen Sie die nachstehenden Links, um weitere Informationen zum Erstellen eines Vorlagen Datenträgers zu finden.

- [Windows-Vorlagen Datenträger vorbereiten](#)
- [Einen Linux-Vorlagen Datenträger](#)

Außerdem benötigen Sie eine Kopie des volumesignaturkatalogs des Datenträgers, um die Schutz Datendatei zu erstellen. Zum Speichern dieser Datei führen Sie den folgenden Befehl auf dem Computer aus, auf dem Sie den Vorlagen Datenträger erstellt haben:

```
Save-VolumeSignatureCatalog -TemplateDiskPath "C:\temp\MyTemplateDisk.vhdx" -VolumeSignatureCatalogPath "C:\temp\MyTemplateDiskCatalog.vsc"
```

Überwachungs Metadaten herunterladen

Für jedes virtualisierungsfabrics, in dem Sie Ihre abgeschirmte VM ausführen möchten, müssen Sie die Überwachungs Metadaten für die HGS-Cluster des Fabrics abrufen. Ihr Hostinganbieter sollte diese Informationen für Sie bereitstellen können.

Wenn Sie sich in einer Unternehmensumgebung befinden und mit dem HGS-Server kommunizieren können, finden Sie die Überwachungs Metadaten unter *http://<hgsclustername>/KeyProtection/Service/Metadata/2014-07/Metadata.XML*

Erstellen einer Datei mit geschützten Daten (PDK)

Geschützte Daten werden erstellt und im Besitz von Mandanten-VM-Besitzern. Sie enthalten Geheimnisse, die zum Erstellen von abgeschirmten VMS erforderlich sind, die vor dem Fabric-Administrator geschützt werden müssen, z. B. das Administrator Kennwort. Geschützte Daten werden so verschlüsselt, dass Sie nur von den HGS-Servern und dem Mandanten entschlüsselt werden können. Nachdem Sie vom Mandanten/VM-Besitzer erstellt wurde, muss die resultierende PDK-Datei in das geschützte Fabric kopiert werden. Weitere Informationen finden Sie unter [Was sind geschützte Daten und warum ist es erforderlich?](#).

Außerdem benötigen Sie eine Antwortdatei für die unbeaufsichtigte Installation (Unattend. XML für Windows, variiert für Linux). Eine Anleitung zum Einbeziehen der Antwortdatei finden Sie unter [Erstellen einer Antwortdatei](#).

Führen Sie die folgenden Cmdlets auf einem Computer aus, auf dem die Remoteserver-Verwaltungstools für abgeschirmte VMS installiert ist. Wenn Sie ein PDK für eine Linux-VM erstellen, müssen Sie dies auf einem Server ausführen, auf dem Windows Server, Version 1709 oder höher, ausgeführt wird.

```
# Create owner certificate, don't lose this!
# The certificate is stored at Cert:\LocalMachine\Shielded VM Local Certificates
$Owner = New-HgsGuardian -Name 'Owner' -GenerateCertificates

# Import the HGS guardian for each fabric you want to run your shielded VM
$Guardian = Import-HgsGuardian -Path C:\HGSGuardian.xml -Name 'TestFabric'

# Create the PDK file
# The "Policy" parameter describes whether the admin can see the VM's console or not
# Use "EncryptionSupported" if you are testing out shielded VMs and want to debug any issues during the
specialization process
New-ShieldingDataFile -ShieldingDataFilePath 'C:\temp\Contoso.pdk' -Owner $Owner -Guardian $Guardian -
VolumeIDQualifier (New-VolumeIDQualifier -VolumeSignatureCatalogFilePath 'C:\temp\MyTemplateDiskCatalog.vsc' -
VersionRule Equals) -WindowsUnattendFile 'C:\unattend.xml' -Policy Shielded
```

Bereitstellen einer abgeschirmten VM auf einem überwachten Host

Kopieren Sie die Vorlagen Datenträger-Datei (serveros.vhdx) und die PDK-Datei (". PDK") auf den überwachten Host, um die Bereitstellung vorzubereiten.

Installieren Sie auf dem überwachten Host das PowerShell-Modul für geschützte Fabric-Tools, das das Cmdlet New-shieldedvm enthält, um den Bereitstellungs Prozess zu vereinfachen. Wenn der überwachte Host auf das Internet zugreifen kann, führen Sie den folgenden Befehl aus:

```
Install-Module GuardedFabricTools -Repository PSGallery -MinimumVersion 1.0.0
```

Sie können das Modul auch auf einen anderen Computer herunterladen, der über Internet Zugriff verfügt, und das resultierende Modul in `C:\Program Files\WindowsPowerShell\Modules` auf dem überwachten Host kopieren.

```
Save-Module GuardedFabricTools -Repository PSGallery -MinimumVersion 1.0.0 -Path C:\temp\
```

Nachdem das Modul installiert wurde, können Sie den abgeschirmten virtuellen Computer bereitstellen.

```
New-ShieldedVM -Name 'MyShieldedVM' -TemplateDiskPath 'C:\temp\MyTemplateDisk.vhdx' -ShieldingDataFilePath
'C:\temp\Contoso.pdk' -Wait
```

Wenn die Antwortdatei für die Schutz Daten Spezialisierungs Werte enthält, können Sie die Ersatzwerte für New-shieldedvm bereitstellen. In diesem Beispiel wird die Antwortdatei mit Platzhalterwerten für eine statische IPv4-Adresse konfiguriert.

```
$specializationValues = @{
    "@IP4Addr-1@" = "192.168.1.10/24"
    "@MacAddr-1@" = "Ethernet"
    "@Prefix-1-1@" = "24"
    "@NextHop-1-1@" = "192.168.1.254"
}
New-ShieldedVM -Name 'MyStaticIPVM' -TemplateDiskPath 'C:\temp\MyTemplateDisk.vhdx' -ShieldingDataFilePath
'C:\temp\Contoso.pdk' -SpecializationValues $specializationValues -Wait
```

Wenn Ihr Vorlagen Datenträger ein Linux-basiertes Betriebssystem enthält, schließen Sie beim Ausführen des Befehls das `-Linux`-Flag ein:

```
New-ShieldedVM -Name 'MyLinuxVM' -TemplateDiskPath 'C:\temp\MyTemplateDisk.vhdx' -ShieldingDataFilePath
'C:\temp\Contoso.pdk' -Wait -Linux
```

Überprüfen Sie den Hilfe Inhalt mithilfe `Get-Help New-ShieldedVM -Full`, um mehr über andere Optionen zu erfahren, die Sie an das Cmdlet übergeben können.

Nachdem die Bereitstellung des virtuellen Computers abgeschlossen ist, wird er in die betriebssystemspezifische Spezialisierungs Phase eingegeben, in der er zur Verwendung bereit ist. Stellen Sie sicher, dass Sie die VM mit einem gültigen Netzwerk verbinden, damit Sie eine Verbindung mit dem virtuellen Computer herstellen können, sobald er ausgeführt wird (mithilfe von RDP, PowerShell, SSH oder Ihrem bevorzugten Verwaltungs Tool).

Ausführen von abgeschirmten VMS auf einem Hyper-V-Cluster

Wenn Sie versuchen, abgeschirmte VMS auf geclusterten überwachten Hosts (mithilfe eines Windows-Failoverclusters) bereitzustellen, können Sie den abgeschirmten virtuellen Computer mit dem folgenden Cmdlet so konfigurieren, dass er hoch verfügbar ist:

```
Add-ClusterVirtualMachineRole -VMName 'MyShieldedVM' -Cluster <Hyper-V cluster name>
```

Der abgeschirmte virtuelle Computer kann nun im Cluster Live migriert werden.

Nächster Schritt

[Bereitstellen eines abgeschirmten mithilfe von VMM](#)

Abgeschirmte VMs für Mandanten: Bereitstellen einer abgeschirmten VM mithilfe von Virtual Machine Manager

09.04.2020 • 2 minutes to read • [Edit Online](#)

Wenn Sie Zugriff auf System Center 2016-Virtual Machine Manager (VMM) haben, können Sie einen abgeschirmten virtuellen Computer bereitstellen, für den bereits eine geschützte VM-Vorlage erstellt wurde.

Verwenden Sie zum Bereitstellen eines abgeschirmten virtuellen Computers in VMM die Anweisungen unter [Bereitstellen einer neuen abgeschirmten VM](#).

Siehe auch

- [Bereitstellen von abgeschirmten VMs](#)
- [Geschütztes Fabric und abgeschirmte VMs](#)

Abgeschirmte VMs für Mandanten: Bereitstellen einer abgeschirmten VM mithilfe von Windows Azure Pack

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2019, Windows Server 2016

Wenn Ihr hostingdienstanbieter dies unterstützt, können Sie Windows Azure Pack verwenden, um eine abgeschirmte VM bereitzustellen.

Führen Sie die folgenden Schritte aus:

1. Abonnieren Sie mindestens einen Plan, der in Windows Azure Pack angeboten wird.
2. Erstellen Sie mithilfe Windows Azure Pack eine abgeschirmte VM.

Verwenden Sie [abgeschirmte virtuelle](#) Computer, die in den folgenden Themen beschrieben werden:

- [Erstellen](#) Sie Schutz Daten (und laden Sie die geschützte Datendatei hoch, wie im zweiten Verfahren im Thema beschrieben).

NOTE

Als Teil der Erstellung von Schutz Daten laden Sie die Datei mit dem Überwachungs Schlüssel herunter. dabei handelt es sich um eine XML-Datei im UTF-8-Format. Ändern Sie die Datei nicht in UTF-16.

- [Erstellen Sie einen abgeschirmten virtuellen Computer](#) mit **schneller** Fassung, über eine geschützte Vorlage oder über eine reguläre Vorlage.

WARNING

Wenn Sie [einen abgeschirmten virtuellen Computer mithilfe einer regulären Vorlage erstellen](#), ist es wichtig zu beachten, dass der virtuelle Computer *nicht geschützt bereitgestellt wird*. Dies bedeutet, dass der Vorlagen Datenträger nicht anhand der Liste der vertrauenswürdigen Datenträger in der geschützten Datendatei überprüft wird, und dass es sich nicht um die geheimen Daten in der Schutz Datendatei handelt. Wenn eine geschützte Vorlage verfügbar ist, empfiehlt es sich, einen abgeschirmten virtuellen Computer mit einer abgeschirmten Vorlage bereitzustellen, um den End-to-End-Schutz ihrer geheimen Schlüssel zu gewährleisten.

- [Konvertieren einer virtuellen Maschine der Generation 2 in eine abgeschirmte virtuelle Maschine](#)

NOTE

Wenn Sie eine virtuelle Maschine in einen abgeschirmten virtuellen Computer konvertieren, werden vorhandene Prüfpunkte und Sicherungen nicht verschlüsselt. Wenn möglich, sollten Sie alte Prüfpunkte löschen, um den Zugriff auf Ihre alten, entschlüsselten Daten zu verhindern.

Siehe auch

- Konfigurationsschritte des hostingdiensteanbieters für geschützte Hosts und abgeschirmte VMS
- Geschütztes Fabric und abgeschirmte VMs

Abgeschirmte VMS: Vorbereiten einer VHD für ein VM-Schutz Hilfsprogramm

09.04.2020 • 4 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

IMPORTANT

Bevor Sie mit diesen Verfahren beginnen, stellen Sie sicher, dass Sie das neueste kumulative Update für Windows Server 2016 installiert haben oder die neuesten Windows 10- [Remoteserver-Verwaltungstools](#) verwenden. Andernfalls funktionieren die Prozeduren nicht.

In diesem Abschnitt werden die Schritte beschrieben, die von einem hostingdienstanbieter ausgeführt werden, um die Unterstützung für die Umstellung vorhandener virtueller

Informationen dazu, wie sich dieses Thema in den Gesamtprozess der Bereitstellung von abgeschirmten VMS einfügt, finden Sie unter [Hosten von Dienst Anbietern Konfigurationsschritte für geschützte Hosts und abgeschirmte VMS](#).

Welche VMs können geschützt werden?

Der Schutz Vorgang für vorhandene VMS ist nur für VMS verfügbar, die die folgenden Voraussetzungen erfüllen:

- Das Gast Betriebssystem ist Windows Server 2012, 2012 R2, 2016 oder eine halbjährliche Kanal Version. Vorhandene virtuelle Linux-Computer können nicht in abgeschirmte VMS konvertiert werden.
- Der virtuelle Computer ist eine VM der Generation 2 (UEFI-Firmware).
- Der virtuelle Computer verwendet keine differenzierenden Datenträger für das Betriebssystem Volume.

Vorbereiten der VHD

1. Erstellen Sie auf einem Computer mit Hyper-V und dem Remoteserver-Verwaltungstools Feature **abgeschirmte VM-Tools** installiert einen neuen virtuellen Computer der Generation 2 mit einer leeren vhdx-Datei, und installieren Sie Windows Server 2016 mithilfe der ISO-Installationsmedien von Windows Server. Diese VM sollte nicht geschützt werden und muss Server Core oder Server mit Desktop Darstellung ausführen.

IMPORTANT

Die VHD für das VM-Schutz Hilfsprogramm **darf nicht** mit den Vorlagen Datenträgern verknüpft sein, die Sie im [hostingdienstanbieter](#) erstellt haben. Wenn Sie einen Vorlagen Datenträger wieder verwenden, wird während des Schutz Vorgangs ein Datenträger Signatur Konflikt festgestellt, da beide Datenträger denselben GPT-Datenträger Bezeichner aufweisen. Sie können dies vermeiden, indem Sie eine neue (leere) VHD erstellen und Windows Server 2016 mithilfe der ISO-Installationsmedien auf diesem Server installieren.

2. Starten Sie den virtuellen Computer, führen Sie alle Setup Schritte aus, und melden Sie sich beim Desktop an. Nachdem Sie überprüft haben, dass sich die VM in einem funktionierenden Zustand befindet, fahren Sie den virtuellen Computer herunter.
3. Führen Sie in einem Windows PowerShell-Fenster mit erhöhten Rechten den folgenden Befehl aus, um die

zuvor erstellte vhdx-Datei als VM-schutzhilfshilf-Daten Träger vorzubereiten. Aktualisieren Sie den Pfad mit dem richtigen Pfad für Ihre Umgebung.

```
Initialize-VMShieldingHelperVHD -Path 'C:\VHD\shieldingHelper.vhdx'
```

4. Nachdem der Befehl erfolgreich abgeschlossen wurde, kopieren Sie die vhdx-Datei in die VMM-Bibliotheks Freigabe. Starten Sie den virtuellen Computer **nicht** erneut aus Schritt 1. Dadurch wird der hilfsprogrammdateienträger beschädigt.
5. Nun können Sie den virtuellen Computer aus Schritt 1 in Hyper-V löschen.

VMM-Host-Überwachungs Server Einstellungen konfigurieren

Öffnen Sie in der VMM-Konsole den Bereich Einstellungen, und wählen Sie dann unter **Allgemein** die Einstellungen des Überwachungs **Diensts** . Am unteren Rand dieses Fensters befindet sich ein Feld, in dem Sie den Speicherort der Hilfs-VHD konfigurieren können. Verwenden Sie die Schaltfläche Durchsuchen, um die VHD aus der Bibliotheks Freigabe auszuwählen. Wenn der Datenträger in der Freigabe nicht angezeigt wird, müssen Sie die Bibliothek in VMM möglicherweise manuell aktualisieren, damit Sie angezeigt wird.

Host Guardian Service Settings

Specify Host Guardian Service and related settings

When you enable the Host Guardian Service on a host, the following URLs will be configured on the host. Virtual Machine Manager (VMM) will also use the Key Protection Server URL as the destination for tenant keys.

Attestation Server URL:

Example: http://contoso.com/Attestation

Key Protection Server URL:

Example: http://contoso.com/KeyProtection

Code Integrity policies

These policies restrict the software that can run on the host. After you click Finish, when you configure properties for a host, you can select the policies to apply to that host, if those policies are in a path that is accessible by the host computer account.

Policies:

| Name | File Path |
|------|-----------|
|------|-----------|

Shielding Helper VHD

Select a VHD that VMM will use for OS volume encryption while shielding existing virtual machines.

Siehe auch

- [Konfigurationsschritte des hostingdienstanbieters für geschützte Hosts und abgeschirmte VMS](#)
- [Geschütztes Fabric und abgeschirmte VMs](#)

Verwalten eines geschützten Fabrics

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

In den folgenden Themen wird beschrieben, wie Sie ein geschütztes Fabric verwalten.

- [Verwalten des Host-Überwachungsdiensts](#)
- [Überlegungen zu Filialen](#)

Siehe auch

- [Bereitstellen eines geschützten Fabrics](#)

Verwalten des Host-Überwachungs Diensts

09.04.2020 • 78 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Der Host-Überwachungsdienst (Host Guardian Service, HGS) ist das Kernstück der geschützten Fabric-Lösung. Er ist dafür verantwortlich, sicherzustellen, dass Hyper-V-Hosts im Fabric dem Host oder Unternehmen bekannt sind und vertrauenswürdige Software ausführen und die Schlüssel verwalten, die zum Starten von abgeschirmten VMS verwendet werden. Wenn ein Mandant beschließt, Sie zu hosten, um die geschützten VMS zu hosten, platziert er seine Vertrauensstellung in Ihrer Konfiguration und Verwaltung des Host-Überwachungs Diensts. Daher ist es sehr wichtig, die bewährten Methoden bei der Verwaltung des Host-Überwachungs Diensts zu befolgen, um die Sicherheit, Verfügbarkeit und Zuverlässigkeit Ihres geschützten Fabrics sicherzustellen. In den Anweisungen in den folgenden Abschnitten werden die häufigsten Betriebsprobleme behandelt, die Administratoren von HGS begegnen.

Einschränken des Administrator Zugriffs auf HGS

Aufgrund der sicherheitssensiblen Natur von HGS ist es wichtig sicherzustellen, dass seine Administratoren sehr vertrauenswürdige Mitglieder Ihrer Organisation sind und im Idealfall von den Administratoren Ihrer Fabric-Ressourcen getrennt werden. Außerdem wird empfohlen, dass Sie nur HGS von sicheren Arbeitsstationen mithilfe von sicheren Kommunikationsprotokollen verwalten, wie z. b. WinRM über HTTPS.

Trennung von Aufgaben

Beim Einrichten von HGS haben Sie die Möglichkeit, eine isolierte Active Directory Gesamtstruktur nur für HGS zu erstellen oder HGS mit einer vorhandenen vertrauenswürdigen Domäne zu verknüpfen. Diese Entscheidung und die Rollen, die Sie den Administratoren in Ihrer Organisation zuweisen, bestimmen die Vertrauensstellungs Grenze für HGS. Wer Zugriff auf HGS hat, egal ob direkt als Administrator oder indirekt als Administrator von etwas anderem (z. b. Active Directory), das die HGS beeinflussen kann, hat Kontrolle über das geschützte Fabric. HGS-Administratoren wählen, welche Hyper-V-Hosts autorisiert sind, abgeschirmte VMS auszuführen und die Zertifikate zu verwalten, die zum Starten von abgeschirmten VMS erforderlich sind. Angreifer oder böswillige Administratoren, die Zugriff auf HGS haben, können mit dieser Leistungsfähigkeit kompromittierte Hosts autorisieren, geschützte VMS auszuführen, einen Denial-of-Service-Angriff durch Entfernen wichtiger Materialien und vieles mehr zu initiieren.

Um dieses Risiko zu vermeiden, wird *dringend* empfohlen, die Überschneidung zwischen den Administratoren Ihrer HGS (einschließlich der Domäne, mit der HGS verknüpft ist) und Hyper-V-Umgebungen einzuschränken. Wenn Sie sicherstellen, dass kein Administrator auf beide Systeme zugreifen kann, müsste ein Angreifer zwei verschiedene Konten von 2 Personen kompromittieren, um seine Aufgabe zum Ändern der HGS-Richtlinien abzuschließen. Dies bedeutet auch, dass die Domänen- und Organisations-Administratoren für die beiden Active Directory Umgebungen nicht dieselbe Person sein sollten und dass HGS dieselbe Active Directory Gesamtstruktur wie Ihre Hyper-V-Hosts verwenden. Jeder Benutzer, der sich selbst Zugriff auf Weitere Ressourcen gewähren kann, stellt ein Sicherheitsrisiko dar.

Verwendung von Just Enough Administration

HGS verfügt über [Just](#) -in-Management-Rollen (Jea), die Sie bei der sicheren Verwaltung unterstützen. Jea unterstützt Sie bei der Delegierung von Administrator Aufgaben an Benutzer ohne Administratorrechte, was bedeutet, dass die Personen, die HGS-Richtlinien verwalten, eigentlich nicht Administratoren des gesamten Computers oder der Domäne sein müssen. Jea schränkt die Befehle ein, die ein Benutzer in einer PowerShell-Sitzung ausführen kann, und verwendet ein temporäres lokales Konto im Hintergrund (eindeutig für jede

Benutzersitzung), um die Befehle auszuführen, die normalerweise eine Erhöhung erfordern.

In HGS werden zwei vorkonfigurierte Jea-Rollen bereitgestellt:

- **HGS-Administratoren** , die es Benutzern ermöglichen, alle HGS-Richtlinien zu verwalten, einschließlich der Autorisierungs Autorisierungs neuer Hosts zum Ausführen geschützter VMS.
- **HGS-Prüfer** , die nur Benutzern das Recht zum Überwachen vorhandener Richtlinien erlauben. Sie können keine Änderungen an der HGS-Konfiguration vornehmen.

Um Jea verwenden zu können, müssen Sie zunächst einen neuen Standardbenutzer erstellen und Sie zu einem Mitglied der Gruppe "HGS-Administratoren" oder "HGS-Prüfer" machen. Wenn Sie `Install-HgsServer` verwendet haben, um eine neue Gesamtstruktur für HGS einzurichten, werden diese Gruppen "*Service Name*Administrators" und "*Service Name*Reviewer" genannt, wobei "*Service Name*" der Netzwerkname des HGS-Clusters ist. Wenn Sie HGS zu einer vorhandenen Domäne hinzugefügt haben, sollten Sie auf die Gruppennamen verweisen, die Sie in `Initialize-HgsServer` angegeben haben.

Erstellen von Standard Benutzern für die Rollen "HGS-Administrator" und "Reviewer"

```
$hgsServiceName = (Get-ClusterResource HgsClusterResource | Get-ClusterParameter DnsName).Value
$adminGroup = $hgsServiceName + "Administrators"
$reviewerGroup = $hgsServiceName + "Reviewers"

New-ADUser -Name 'hgsadmin01' -AccountPassword (Read-Host -AsSecureString -Prompt 'HGS Admin Password') -
ChangePasswordAtLogon $false -Enabled $true
Add-ADGroupMember -Identity $adminGroup -Members 'hgsadmin01'

New-ADUser -Name 'hgsreviewer01' -AccountPassword (Read-Host -AsSecureString -Prompt 'HGS Reviewer Password') -
ChangePasswordAtLogon $false -Enabled $true
Add-ADGroupMember -Identity $reviewerGroup -Members 'hgsreviewer01'
```

Überwachen von Richtlinien mit der Reviewer-Rolle

Führen Sie auf einem Remote Computer mit Netzwerk Konnektivität mit HGS die folgenden Befehle in PowerShell aus, um die Jea-Sitzung mit den Reviewer-Anmelde Informationen einzugeben. Beachten Sie Folgendes: da das Reviewer-Konto nur ein Standardbenutzer ist, kann es nicht für reguläre Windows PowerShell-Remoting, Remotedesktop Zugriff auf HGS usw. verwendet werden.

```
Enter-PSSession -ComputerName <hgsnode> -Credential '<hgsdomain>\hgsreviewer01' -ConfigurationName
'microsoft.windows.hgs'
```

Sie können dann überprüfen, welche Befehle in der Sitzung mit `Get-Command` zulässig sind, und alle zulässigen Befehle zum Überwachen der Konfiguration ausführen. Im folgenden Beispiel überprüfen wir, welche Richtlinien auf HGS aktiviert sind.

```
Get-Command

Get-HgsAttestationPolicy
```

Geben Sie den Befehl `Exit-PSSession` oder den zugehörigen Alias ein, `exit` , wenn Sie mit der Jea-Sitzung gearbeitet haben.

Hinzufügen einer neuen Richtlinie zu HGS mithilfe der Administrator Rolle

Um eine Richtlinie tatsächlich zu ändern, müssen Sie eine Verbindung mit dem Jea-Endpunkt mit einer Identität herstellen, die zur Gruppe "hgsadministrators" gehört. Im folgenden Beispiel wird gezeigt, wie Sie eine neue Code Integritätsrichtlinie in HGS kopieren und mit Jea registrieren können. Die Syntax unterscheidet sich möglicherweise von ihrer Verwendung. Dies dient dazu, einige der Einschränkungen in Jea zu erfüllen, wie z. b.

keinen Zugriff auf das vollständige Dateisystem.

```
$cipolicy = Get-Item "C:\temp\cipolicy.p7b"
$session = New-PSSession -ComputerName <hgsnode> -Credential '<hgsdomain>\hgsadmin01' -ConfigurationName
'microsoft.windows.hgs'
Copy-Item -Path $cipolicy -Destination 'User:' -ToSession $session

# Now that the file is copied, we enter the interactive session to register it with HGS
Enter-PSSession -Session $session
Add-HgsAttestationCiPolicy -Name 'New CI Policy via JEA' -Path 'User:\cipolicy.p7b'

# Confirm it was added successfully
Get-HgsAttestationPolicy -PolicyType CiPolicy

# Finally, remove the PSSession since it is no longer needed
Exit-PSSession
Remove-PSSession -Session $session
```

Überwachen von HGS

Ereignis Quellen und Weiterleitung

Ereignisse von HGS werden im Windows-Ereignisprotokoll unter 2 Quellen angezeigt:

- **Hostguardianservice-Nachweis**
- **Hostguardianservice-keyprotection**

Sie können diese Ereignisse anzeigen, indem Sie Ereignisanzeige öffnen und zu "Microsoft-Windows-hostguardianservice-Attestation" und "Microsoft-Windows-hostguardianservice-keyprotection" navigieren.

In einer großen Umgebung ist es häufig vorzuziehen, Ereignisse an einen zentralen Windows-Ereignis Sammler weiterzuleiten, um die Analyse der Ereignisse zu vereinfachen. Weitere Informationen finden Sie in der [Dokumentation zur Windows-Ereignis Weiterleitung](#).

Verwenden von System Center Operations Manager

Sie können auch System Center 2016-Operations Manager verwenden, um HGS und die überwachten Hosts zu überwachen. Der geschützte Fabric-Management Pack verfügt über Ereignis Monitore, die auf häufige Fehlkonfigurationen überprüfen können, die zu Ausfallzeiten von Rechenzentren führen können, einschließlich Hosts, die keine Nachrichten übergeben, und HGS-Server, die Fehler melden

[Installieren und konfigurieren Sie zunächst SCOM 2016](#) , und [Laden Sie die geschützte Fabric-Management Pack herunter](#). Das enthaltene Management Pack Handbuch erläutert, wie Sie die Management Pack konfigurieren und den Bereich Ihrer Monitore verstehen.

Sichern und Wiederherstellen von HGS

Planen der Notfall Wiederherstellung

Beim Entwerfen Ihrer Notfall Wiederherstellungs Pläne ist es wichtig, die besonderen Anforderungen des Host-Überwachungs Diensts in Ihrem geschützten Fabric zu beachten. Wenn Sie einige oder alle ihrer HGS-Knoten verlieren, treten möglicherweise unmittelbare Verfügbarkeits Probleme auf, die verhindern, dass Benutzer ihre abgeschirmten VMs starten. In einem Szenario, in dem Sie den gesamten HGS-Cluster verlieren, benötigen Sie vollständige Sicherungen der HGS-Konfiguration, um den HGS-Cluster wiederherstellen und den normalen Betrieb fortsetzen zu können. In diesem Abschnitt werden die erforderlichen Schritte für die Vorbereitung eines solchen Szenarios beschrieben.

Zuerst ist es wichtig zu verstehen, welche Informationen zu HGS für die Sicherungskopie wichtig sind. HGS behält verschiedene Informationen bei, mit denen ermittelt werden kann, welche Hosts zum Ausführen geschützter VMS

autorisiert sind. Dazu zählen:

1. Active Directory Sicherheits-IDs für die Gruppen mit vertrauenswürdigen Hosts (bei Verwendung Active Directory Attestation);
2. Eindeutige TPM-IDs für jeden Host in Ihrer Umgebung
3. TPM-Richtlinien für jede eindeutige Konfiguration des Hosts immer
4. Code Integritäts Richtlinien, die bestimmen, welche Software auf den Hosts ausgeführt werden darf.

Diese Nachweis Artefakte müssen mit den Administratoren Ihres hostingfabrics koordiniert werden, um diese Informationen nach einem Notfall wiederholen zu können.

Außerdem erfordert HGS Zugriff auf zwei oder mehr Zertifikate, die zum Verschlüsseln und Signieren der zum Starten einer abgeschirmten VM erforderlichen Informationen (die Schlüssel Schutzvorrichtung) benötigt werden. Diese Zertifikate sind bekannt (von den Besitzern von abgeschirmten VMS verwendet, um Ihr Fabric zum Ausführen Ihrer virtuellen Computer zu autorisieren) und müssen nach einem Notfall wieder hergestellt werden, um eine nahtlose Wiederherstellung zu ermöglichen. Wenn Sie HGS nicht mit denselben Zertifikaten nach einem Notfall wiederherstellen, muss jeder virtuelle Computer aktualisiert werden, um die neuen Schlüssel zum Entschlüsseln Ihrer Informationen zu autorisieren. Aus Sicherheitsgründen kann nur der Besitzer des virtuellen Computers die VM-Konfiguration aktualisieren, um diese neuen Schlüssel zu autorisieren. Dies bedeutet, dass die Wiederherstellung Ihrer Schlüssel nach einem Notfall dazu führt, dass jeder VM-Besitzer Maßnahmen ergreifen muss, damit die virtuellen Computer erneut ausgeführt werden.

Vorbereitung auf die schlechteste

Um einen kompletten Verlust von HGS vorzubereiten, müssen Sie zwei Schritte ausführen:

1. Sichern der HGS-Nachweis Richtlinien
2. Sichern der HGS-Schlüssel

Anweisungen zum Ausführen dieser beiden Schritte finden Sie im Abschnitt [Sichern von HGS](#) .

Außerdem wird empfohlen, aber nicht erforderlich, dass Sie die Liste der Benutzer sichern, die zum Verwalten von HGS in der Active Directory Domäne oder Active Directory selbst autorisiert sind.

Sicherungen sollten regelmäßig ausgeführt werden, um sicherzustellen, dass die Informationen auf dem neuesten Stand sind und sicher gespeichert werden, um Manipulationen oder Diebstähle zu vermeiden.

Es wird **nicht empfohlen** , ein gesamtes System Abbild eines HGS-Knotens zu sichern oder wiederherzustellen. Wenn Sie den gesamten Cluster verloren haben, besteht die bewährte Methode darin, einen neuen HGS-Knoten einzurichten und nur den HGS-Status und nicht das gesamte Server Betriebssystem wiederherzustellen.

Wiederherstellung nach dem Verlust eines Knotens

Wenn Sie einen oder mehrere Knoten (aber nicht jeden Knoten) in Ihrem HGS-Cluster verlieren, können Sie dem [Cluster einfach Knoten hinzufügen](#) , indem Sie die Anleitungen im Bereitstellungs Handbuch befolgen. Die Nachweis Richtlinien werden automatisch synchronisiert, ebenso wie alle Zertifikate, die HGS als PFX-Dateien mit begleitenden Kenn Wörtern bereitgestellt wurden. Für Zertifikate, die zu HGS mithilfe eines Fingerabdrucks (nicht exportierbar und Hardware gestützte Zertifikate, häufig) hinzugefügt werden, müssen Sie sicherstellen, dass jeder neue Knoten Zugriff auf den privaten Schlüssel jedes Zertifikats hat.

Wiederherstellung nach dem Verlust des gesamten Clusters

Wenn der gesamte HGS-Cluster ausfällt und Sie nicht wieder online geschaltet werden können, müssen Sie HGS aus einer Sicherung wiederherstellen. Das Wiederherstellen von HGS aus einer Sicherung umfasst zunächst das Einrichten eines neuen HGS-Clusters gemäß der [Anleitung im Bereitstellungs Handbuch](#). Es wird dringend empfohlen, den gleichen Cluster Namen zu verwenden, wenn die Recovery-HGS-Umgebung eingerichtet wird, um die Namensauflösung von Hosts zu unterstützen. Wenn Sie denselben Namen verwenden, müssen Sie die Hosts mit neuen Nachweis- und Schlüsselschutz-URLs nicht neu konfigurieren. Wenn Sie Objekte in den Active Directory Domänen Sicherungs-HGS wieder hergestellt haben, wird empfohlen, vor dem Initialisieren des HGS-Servers die Objekte zu entfernen, die den HGS-Cluster, die Computer, das Dienst Konto und die Jea-Gruppen darstellen.

Nachdem Sie den ersten HGS-Knoten eingerichtet haben (z. b. installiert und initialisiert), befolgen Sie die Verfahren unter Wiederherstellen [von HGS aus einer Sicherung](#) , um die Nachweis Richtlinien und die öffentliche Hälfte der Schlüsselschutz Zertifikate wiederherzustellen. Die privaten Schlüssel für Ihre Zertifikate müssen manuell gemäß der Anleitung Ihres Zertifikat Anbieters wieder hergestellt werden (z. b. Importieren des Zertifikats in Windows oder Konfigurieren des Zugriffs auf HSM-gestützte Zertifikate). Nachdem Sie den ersten Knoten eingerichtet haben, können Sie weiterhin [zusätzliche Knoten auf dem Cluster installieren](#) , bis Sie die gewünschte Kapazität und Resilienz erreicht haben.

Sichern von HGS

Der HGS-Administrator sollte in regelmäßigen Abständen für die Sicherung von HGS verantwortlich sein. Eine komplette Sicherung enthält vertrauliche Schlüsselmaterial, die entsprechend gesichert werden müssen. Sollte eine nicht vertrauenswürdige Entität Zugriff auf diese Schlüssel erhalten, können Sie diese Informationen verwenden, um eine bössartige HGS-Umgebung zum Zweck der Gefährdung von abgeschirmten VMS einzurichten.

Sichern der Nachweis Richtlinien Um die Richtlinien für den HGS-Nachweis zu sichern, führen Sie den folgenden Befehl auf einem beliebigen funktionierenden HGS-Server Knoten aus. Sie werden aufgefordert, ein Kennwort anzugeben. Dieses Kennwort wird zum Verschlüsseln aller Zertifikate verwendet, die zu HGS hinzugefügt werden, indem eine PFX-Datei (anstelle eines Zertifikat Fingerabdrucks) verwendet wird.

```
Export-HgsServerState -Path C:\temp\HGSBackup.xml
```

NOTE

Wenn Sie einen vom Administrator vertrauenswürdigen Nachweis verwenden, müssen Sie die Mitgliedschaft in den Sicherheitsgruppen, die von HGS zum Autorisieren von überwachten Hosts verwendet werden, separat sichern. HGS sichert nur die SID der Sicherheitsgruppen, nicht die darin enthaltenen Mitgliedschaften. Wenn diese Gruppen während eines Notfalls verloren gehen, müssen Sie die Gruppe (n) neu erstellen und jeden überwachten Host erneut hinzufügen.

Sichern von Zertifikaten

Der `Export-HgsServerState` -Befehl sichert alle PFX-basierten Zertifikate, die zu dem Zeitpunkt, zu dem der Befehl ausgeführt wird, den HGS hinzugefügt werden. Wenn Sie HGS Zertifikate mithilfe eines Fingerabdrucks (typisch für nicht exportierbare und Hardware gestützte Zertifikate) hinzugefügt haben, müssen Sie die privaten Schlüssel für Ihre Zertifikate manuell sichern. Um zu ermitteln, welche Zertifikate bei HGS registriert sind und manuell gesichert werden müssen, führen Sie den folgenden PowerShell-Befehl auf einem beliebigen funktionierenden HGS-Server Knoten aus.

```
Get-HgsKeyProtectionCertificate | Where-Object { $_.CertificateData.GetType().Name -eq 'CertificateReference' } | Format-Table Thumbprint, @{ Label = 'Subject'; Expression = { $_.CertificateData.Certificate.Subject } }
```

Für jedes der aufgeführten Zertifikate müssen Sie den privaten Schlüssel manuell sichern. Wenn Sie ein softwarebasiertes Zertifikat verwenden, das nicht exportierbar ist, wenden Sie sich an die Zertifizierungsstelle, um sicherzustellen, dass Sie über eine Sicherung Ihres Zertifikats verfügen, und/oder können Sie bei Bedarf neu ausstellen. Bei Zertifikaten, die in Hardware Sicherheits Modulen erstellt und gespeichert werden, sollten Sie sich in der Dokumentation zu Ihrem Gerät über die Planung der Notfall Wiederherstellung informieren.

Sie sollten die Zertifikat Sicherungen zusammen mit den Nachweis Richtlinien Sicherungen an einem sicheren Ort speichern, damit beide Teile zusammen wieder hergestellt werden können.

Zusätzliche Konfiguration für die Sicherungskopie

Der gesicherte HGS-Serverstatus enthält nicht den Namen Ihres HGS-Clusters, Informationen aus Active Directory oder SSL-Zertifikate, die zum Sichern der Kommunikation mit den HGS-APIs verwendet werden. Diese

Einstellungen sind wichtig, um Konsistenz zu gewährleisten, aber nicht wichtig, um Ihren HGS-Cluster nach einem Notfall wieder online zu schalten.

Um den Namen des HGS-dienstanweises aufzuzeichnen, führen Sie `Get-HgsServer` aus, und notieren Sie sich den flachen Namen in den URLs für den Nachweis und den Schlüsselschutz. Wenn die Nachweis-URL z. B. "<http://hgs.contoso.com/Attestation>" lautet, ist "HGS" der Name des HGS-dienstanweises.

Die von HGS verwendete Active Directory Domäne sollte wie jede andere Active Directory Domäne verwaltet werden. Wenn Sie HGS nach einem Notfall wiederherstellen, müssen Sie nicht unbedingt die exakten Objekte neu erstellen, die in der aktuellen Domäne vorhanden sind. Allerdings wird die Wiederherstellung vereinfacht, wenn Sie Active Directory sichern und eine Liste der Jeo-Benutzer, die zur Verwaltung des Systems autorisiert sind, sowie die Mitgliedschaft von Sicherheitsgruppen, die vom Administrator vertrauenswürdigen Nachweis verwendet werden, zum Autorisieren von überwachten Hosts erhalten.

Führen Sie den folgenden Befehl in PowerShell aus, um den Fingerabdruck der SSL-Zertifikate zu identifizieren, die für HGS konfiguriert sind. Anschließend können Sie die SSL-Zertifikate gemäß den Anweisungen Ihres Zertifikat Anbieters sichern.

```
Get-WebBinding -Protocol https | Select-Object certificateHash
```

Wiederherstellen von HGS aus einer Sicherung

In den folgenden Schritten wird beschrieben, wie Sie die HGS-Einstellungen aus einer Sicherung wiederherstellen. Die Schritte sind für beide Situationen relevant, in denen Sie versuchen, Änderungen an Ihren bereits vorhandenen HGS-Instanzen rückgängig zu machen, und wenn Sie nach einem vollständigen Verlust der vorherigen Instanz einen neuen HGS-Cluster einrichten.

Einrichten eines Ersetzungs-HGS-Clusters

Bevor Sie HGS wiederherstellen können, benötigen Sie einen initialisierten HGS-Cluster, auf dem Sie die Konfiguration wiederherstellen können. Wenn Sie einfach Einstellungen importieren, die versehentlich in einen vorhandenen (laufenden) Cluster gelöscht wurden, können Sie diesen Schritt überspringen. Wenn Sie nach einem kompletten Verlust von HGS wiederherstellen, müssen Sie mindestens einen HGS-Knoten installieren und initialisieren, indem Sie die [Anweisungen im Bereitstellungs Handbuch](#) befolgen.

Insbesondere müssen Sie die folgenden Schritte ausführen:

1. [Einrichten der HGS-Domäne](#) oder einbinden von HGS in eine vorhandene Domäne
2. [Initialisieren Sie den HGS-Server](#) mit Ihren vorhandenen Schlüsseln *oder* einem Satz von temporären Schlüsseln. Sie können [die temporären Schlüssel](#) nach dem Importieren Ihrer eigentlichen Schlüssel aus den HGS-Sicherungsdateien entfernen.
3. [Importieren Sie die HGS-Einstellungen](#) aus der Sicherung, um die vertrauenswürdigen Host Gruppen, Code Integritäts Richtlinien, TPM-Baselines und TPM-IDs wiederherzustellen.

TIP

Der neue HGS-Cluster muss nicht die gleichen Zertifikate, den gleichen Dienstnamen oder die gleiche Domäne wie die HGS-Instanz verwenden, von der aus die Sicherungsdatei exportiert wurde.

Importieren von Einstellungen aus einer Sicherung

Führen Sie den folgenden Befehl auf einem initialisierten HGS-Server Knoten aus, um Nachweis Richtlinien, PFX-basierte Zertifikate und die öffentlichen Schlüssel von nicht-PFX-Zertifikaten auf Ihrem HGS-Knoten aus einer Sicherungsdatei wiederherzustellen. Sie werden aufgefordert, das Kennwort einzugeben, das Sie beim Erstellen der Sicherung angegeben haben.

```
Import-HgsServerState -Path C:\Temp\HGSBackup.xml
```

Wenn Sie nur admin-Trusted Nachweis-Richtlinien oder TPM-vertrauenswürdige Nachweis Richtlinien importieren möchten, können Sie dazu die `-ImportActiveDirectoryModeState` oder `-ImportTpmModeState` Flags für [Import-hgsserverstate](#) angeben.

Stellen Sie sicher, dass das neueste kumulative Update für Windows Server 2016 installiert ist, bevor Sie `Import-HgsServerState` ausführen. Wenn dies nicht der Fall ist, kann ein Import Fehler auftreten.

NOTE

Wenn Sie Richtlinien auf einem vorhandenen HGS-Knoten wiederherstellen, auf dem bereits eine oder mehrere dieser Richtlinien installiert sind, wird im Import Befehl ein Fehler für jede doppelte Richtlinie angezeigt. Dies ist ein erwartetes Verhalten und kann in den meisten Fällen problemlos ignoriert werden.

Neuinstallation privater Schlüssel für Zertifikate

Wenn eines der Zertifikate, die auf dem HGS verwendet werden, von dem die Sicherung erstellt wurde, mithilfe von Fingerabdrücken hinzugefügt wurde, wird nur der öffentliche Schlüssel dieser Zertifikate in die Sicherungsdatei eingeschlossen. Dies bedeutet, dass Sie für jedes dieser Zertifikate manuell installieren und/oder Zugriff auf die privaten Schlüssel gewähren müssen, bevor HGS Anforderungen von Hyper-V-Hosts bedienen kann. Welche Aktionen zum Durchführen dieses Schritts erforderlich sind, hängt davon ab, wie das Zertifikat ursprünglich ausgestellt wurde. Bei softwaregestützten Zertifikaten, die von einer Zertifizierungsstelle ausgestellt werden, müssen Sie sich an Ihre Zertifizierungsstelle wenden, um den privaten Schlüssel zu erhalten und auf **jedem** HGS-Knoten gemäß Ihren Anweisungen zu installieren. Wenn Ihre Zertifikate auf Hardware basieren, müssen Sie auch die Dokumentation Ihres Hardware Sicherheitsmodul-Herstellers aufrufen, um die erforderlichen Treiber auf den einzelnen HGS-Knoten zu installieren, um eine Verbindung mit dem HSM herzustellen und jedem Computer Zugriff auf den privaten Schlüssel zu gewähren.

Zur Erinnerung: Zertifikate, die HGS mithilfe von Fingerabdrücken hinzugefügt werden, erfordern eine manuelle Replikation der privaten Schlüssel für jeden Knoten. Sie müssen diesen Schritt auf jedem zusätzlichen Knoten wiederholen, den Sie dem wiederhergestellten HGS-Cluster hinzufügen.

Überprüfen der importierten Nachweis Richtlinien

Nachdem Sie die Einstellungen aus einer Sicherung importiert haben, wird empfohlen, alle importierten Richtlinien mithilfe von `Get-HgsAttestationPolicy` genau zu überprüfen, um sicherzustellen, dass nur die Hosts, denen Sie Vertrauen, dass Sie abgeschirmte VMS ausführen, erfolgreich bestätigt werden können. Wenn Sie Richtlinien finden, die nicht mehr dem Sicherheitsstatus entsprechen, können Sie [diese deaktivieren oder entfernen](#).

Ausführen der Diagnose zum Überprüfen des Systemstatus

Nachdem Sie die Einrichtung und Wiederherstellung des Status des HGS-Knotens abgeschlossen haben, sollten Sie das HGS-Diagnosetool ausführen, um den Status des Systems zu überprüfen. Führen Sie hierzu den folgenden Befehl auf dem HGS-Knoten aus, auf dem Sie die Konfiguration wieder hergestellt haben:

```
Get-HgsTrace -RunDiagnostics
```

Wenn das "Gesamtergebnis" nicht "Pass" ist, sind zusätzliche Schritte erforderlich, um die Konfiguration des Systems abzuschließen. Überprüfen Sie die in den untertests gemeldeten Meldungen, bei denen weitere Informationen aufgetreten sind.

Patching von HGS

Es ist wichtig, die Knoten des Host-Überwachungs Diensts auf dem neuesten Stand zu halten, indem Sie das

aktuellste kumulative Update installieren. Wenn Sie einen neuen HGS-Knoten einrichten, wird dringend empfohlen, dass Sie alle verfügbaren Updates installieren, bevor Sie die HGS-Rolle installieren oder konfigurieren. Dadurch wird sichergestellt, dass neue oder geänderte Funktionen sofort wirksam werden.

Beim Patchen ihres geschützten Fabrics wird dringend empfohlen, zuerst *alle* Hyper-V-Hosts **vor dem Upgrade von HGS** zu aktualisieren. Dadurch wird sichergestellt, dass alle Änderungen an den Nachweis Richtlinien auf den HGS vorgenommen werden, *nachdem* die Hyper-V-Hosts aktualisiert wurden, um die für Sie erforderlichen Informationen bereitzustellen. Wenn das Verhalten von Richtlinien durch ein Update geändert wird, werden Sie nicht automatisch aktiviert, um die Unterbrechung Ihres Fabrics zu vermeiden. Diese Updates erfordern, dass Sie die Anweisungen im folgenden Abschnitt befolgen, um die neuen oder geänderten Nachweis Richtlinien zu aktivieren. Wir empfehlen Ihnen, die Anmerkungen zu dieser Version für Windows Server und alle kumulativen Updates zu lesen, die Sie installieren, um zu prüfen, ob die Richtlinien Updates erforderlich sind.

Updates, die die Richtlinien Aktivierung erfordern

Wenn ein Update für HGS das Verhalten einer Nachweis Richtlinie einführt oder erheblich ändert, ist ein zusätzlicher Schritt erforderlich, um die geänderte Richtlinie zu aktivieren. Richtlinien Änderungen werden nur nach dem Exportieren und Importieren des HGS-Zustands festgesetzt. Sie sollten nur die neuen oder geänderten Richtlinien aktivieren, nachdem Sie das kumulative Update auf alle Hosts und alle HGS-Knoten in Ihrer Umgebung angewendet haben. Nachdem jeder Computer aktualisiert wurde, führen Sie die folgenden Befehle auf einem beliebigen HGS-Knoten aus, um den Upgradevorgang zu initiieren:

```
$password = Read-Host -AsSecureString -Prompt "Enter a temporary password"
Export-HgsServerState -Path .\temporaryExport.xml -Password $password
Import-HgsServerState -Path .\temporaryExport.xml -Password $password
```

Wenn eine neue Richtlinie eingeführt wurde, wird Sie standardmäßig deaktiviert. Um die neue Richtlinie zu aktivieren, suchen Sie Sie zuerst in der Liste der Microsoft-Richtlinien (mit dem Präfix "HGS_"), und aktivieren Sie Sie dann mit den folgenden Befehlen:

```
Get-HgsAttestationPolicy

Enable-HgsAttestationPolicy -Name <Hgs_NewPolicyName>
```

Verwalten von Nachweis Richtlinien

HGS verwaltet mehrere Nachweis Richtlinien, die die Mindestanzahl von Anforderungen definieren, die ein Host erfüllen muss, um als "fehlerfrei" eingestuft zu werden, und für die das Ausführen von abgeschirmten VMS zugelassen ist. Einige dieser Richtlinien werden von Microsoft definiert, andere werden von Ihnen hinzugefügt, um die zulässigen Code Integritäts Richtlinien, TPM-Baselines und Hosts in Ihrer Umgebung zu definieren. Eine regelmäßige Wartung dieser Richtlinien ist erforderlich, um sicherzustellen, dass Hosts beim Aktualisieren und ersetzen weiterhin ordnungsgemäß getestet werden können, und um sicherzustellen, dass nicht vertrauenswürdige Hosts oder Konfigurationen nicht erfolgreich getestet werden können.

Für den Administrator vertrauenswürdigen Nachweis gibt es nur eine Richtlinie, die bestimmt, ob ein Host fehlerfrei ist: Mitgliedschaft in einer bekannten, vertrauenswürdigen Sicherheitsgruppe. Der TPM-Nachweis ist komplizierter und umfasst verschiedene Richtlinien, mit denen der Code und die Konfiguration eines Systems gemessen werden können, bevor festgestellt wird, ob es fehlerfrei ist.

Ein einzelner HGS kann gleichzeitig mit Active Directory- und TPM-Richtlinien konfiguriert werden, aber der Dienst überprüft nur die Richtlinien für den aktuellen Modus, für den er konfiguriert ist, wenn ein Host versucht, die Tests zu testen. Führen Sie `Get-HgsServer` aus, um den Modus des HGS-Servers zu überprüfen.

Standardrichtlinien

Für den TPM-vertrauenswürdigen Nachweis gibt es mehrere integrierte Richtlinien, die auf HGS konfiguriert sind.

Einige dieser Richtlinien sind "gesperrt", was bedeutet, dass Sie aus Sicherheitsgründen nicht deaktiviert werden können. In der folgenden Tabelle wird der Zweck jeder Standard Richtlinie erläutert.

| RICHTLINIENNAME | ZWECK |
|--------------------------------|---|
| Hgs_SecureBootEnabled | Erfordert, dass für Hosts der sichere Start aktiviert ist. Dies ist erforderlich, um die Start Binärdateien und andere UEFI-Locked-Einstellungen zu messen. |
| Hgs_UefiDebugDisabled | Stellt sicher, dass für Hosts kein Kernel Debugger aktiviert ist. Benutzermodus-debuggger werden mit Code Integritäts Richtlinien blockiert. |
| Hgs_SecureBootSettings | Negative Richtlinie, um sicherzustellen, dass die Hosts mindestens einer (vom Administrator definierten) TPM-Baseline entsprechen. |
| Hgs_CiPolicy | Negative Richtlinie, um sicherzustellen, dass die Hosts eine der Administrator definierten CI-Richtlinien verwenden. |
| Hgs_HypervisorEnforcedCiPolicy | Erfordert, dass die Code Integritätsrichtlinie vom Hypervisor erzwungen wird. Wenn Sie diese Richtlinie deaktivieren, wird der Schutz vor kernelmodesintegritäts-Richtlinien Angriffen geschwächt. |
| Hgs_FullBoot | Sicherstellen, dass der Host nicht aus dem Standbymodus oder Ruhezustand fortgesetzt wurde Hosts müssen ordnungsgemäß neu gestartet oder heruntergefahren werden, um diese Richtlinie zu übergeben. |
| Hgs_VsmIdkPresent | Erfordert, dass virtualisierungsbasierte Sicherheit auf dem Host ausgeführt wird. Das idk stellt den Schlüssel dar, der zum Verschlüsseln von Informationen erforderlich ist, die zurück an den sicheren Speicherbereich des Hosts gesendet werden. |
| Hgs_PageFileEncryptionEnabled | Erfordert, dass Auslagerungs Dateien auf dem Host verschlüsselt wird. Wenn Sie diese Richtlinie deaktivieren, kann es zu Informations Informationen kommen, wenn eine unverschlüsselte ausseitendatei auf Mandanten Geheimnisse überprüft wird. |
| Hgs_BitLockerEnabled | Erfordert, dass BitLocker auf dem Hyper-V-Host aktiviert ist. Diese Richtlinie ist aus Leistungsgründen standardmäßig deaktiviert und wird nicht empfohlen, Sie zu aktivieren. Diese Richtlinie hat keine Auswirkungen auf die Verschlüsselung der abgeschirmten VMs selbst. |
| Hgs_IommuEnabled | Erfordert, dass der Host über ein IOMMU-Gerät verfügt, das verwendet wird, um Angriffe durch direkten Speicherzugriff zu verhindern. Wenn Sie diese Richtlinie deaktivieren und Hosts ohne IOMMU-Aktivierung verwenden, können Sie Mandanten-VM-Schlüssel für direkte Speicher Angriffe verfügbar machen. |
| Hgs_NoHibernation | Erfordert, dass der Ruhezustand auf dem Hyper-V-Host deaktiviert wird. Durch die Deaktivierung dieser Richtlinie können Hosts den geschützten VM-Speicher in einer unverschlüsselten Ruhe Zustands Datei speichern. |

| RICHTLINIENNAME | ZWECK |
|-----------------------|---|
| Hgs_NoDumps | Erfordert, dass Speicher Abbilder auf dem Hyper-V-Host deaktiviert werden. Wenn Sie diese Richtlinie deaktivieren, empfiehlt es sich, die dumpverschlüsselung zu konfigurieren, um zu verhindern, dass geschützter VM-Speicher in unverschlüsselten Absturz Abbild Dateien gespeichert wird. |
| Hgs_DumpEncryption | Erfordert, dass Speicher Abbilder, die auf dem Hyper-V-Host aktiviert sind, mit einem Verschlüsselungsschlüssel verschlüsselt werden, der von HGS als vertrauenswürdig eingestuft wird. Diese Richtlinie gilt nicht, wenn Abbilder auf dem Host nicht aktiviert sind. Wenn diese Richtlinie und <i>HGS_nodumps</i> deaktiviert sind, kann der geschützte VM-Speicher in einer unverschlüsselten Dumpdatei gespeichert werden. |
| Hgs_DumpEncryptionKey | Eine negative Richtlinie zum sicherstellen, dass Hosts, die für das Zulassen von Speicher Abbildern konfiguriert sind, einen vom Administrator definierten Verschlüsselungsschlüssel für die Dumpdatei verwendet Diese Richtlinie gilt nicht, wenn <i>HGS_dumpencryption</i> deaktiviert ist. |

Autorialisieren von neuen überwachten Hosts

Um einen neuen Host zu einem überwachten Host zu autorisieren (z. b. erfolgreich), müssen die HGS dem Host Vertrauen und (bei Konfiguration für die Verwendung des TPM-vertrauenswürdigen Attestation) die darauf laufende Software als vertrauenswürdig einstufen. Die Schritte zum Autorisieren eines neuen Hosts unterscheiden sich je nach Nachweis Modus, für den HGS derzeit konfiguriert ist. Führen Sie `Get-HgsServer` auf einem beliebigen HGS-Knoten aus, um den Nachweis Modus für Ihr überwachtes Fabric zu überprüfen.

Softwarekonfiguration

Stellen Sie auf dem neuen Hyper-V-Host sicher, dass Windows Server 2016 Datacenter Edition installiert ist. Windows Server 2016 Standard kann keine abgeschirmten VMs in einem geschützten Fabric ausführen. Auf dem Host ist möglicherweise Desktop Darstellung oder Server Core installiert.

Auf dem Server mit Desktop Darstellung und Server Core müssen Sie die Hyper-v-und Host-Überwachungs Server-Hyper-v-Unterstützungs Server Rollen installieren:

```
Install-WindowsFeature Hyper-V, HostGuardian -IncludeManagementTools -Restart
```

Admin-vertrauenswürdiger Nachweis

Wenn Sie einen neuen Host bei der Verwendung von Administrator vertrauenswürdigem Nachweis in HGS registrieren möchten, müssen Sie ihn zunächst zu einer Sicherheitsgruppe in der Domäne hinzufügen, mit der er verknüpft ist. In der Regel verfügt jede Domäne über eine Sicherheitsgruppe für geschützte Hosts. Wenn Sie diese Gruppe bereits bei HGS registriert haben, müssen Sie nur den Host neu starten, um die Gruppenmitgliedschaft zu aktualisieren.

Sie können überprüfen, welche Sicherheitsgruppen von HGS als vertrauenswürdig eingestuft werden, indem Sie den folgenden Befehl ausführen:

```
Get-HgsAttestationHostGroup
```

Zum Registrieren einer neuen Sicherheitsgruppe bei HGS erfassen Sie zuerst die Sicherheits-ID (SID) der Gruppe in der Host Domäne und registrieren die SID bei HGS.

```
Add-HgsAttestationHostGroup -Name "Contoso Guarded Hosts" -Identifier "S-1-5-21-3623811015-3361044348-30300820-1013"
```

Anweisungen zum Einrichten der Vertrauensstellung zwischen der Host Domäne und den HGS finden Sie im Bereitstellungs Handbuch.

TPM-vertrauenswürdiger Nachweis

Wenn HGS im TPM-Modus konfiguriert ist, müssen Hosts alle gesperrten Richtlinien und aktivierten Richtlinien, die mit dem Präfix "Hgs_" als Präfix versehen sind, sowie mindestens eine TPM-Baseline, TPM-ID und Code Integritätsrichtlinie übergeben. Jedes Mal, wenn Sie einen neuen Host hinzufügen, müssen Sie die neue TPM-ID bei HGS registrieren. Solange der Host dieselbe Software (und die gleiche Code Integritätsrichtlinie angewendet) und die TPM-Baseline als einen anderen Host in Ihrer Umgebung ausführen, müssen Sie keine neuen CI-Richtlinien oder Basis Linien hinzufügen.

Hinzufügen des TPM-Bezeichners für einen neuen Host Führen Sie auf dem neuen Host den folgenden Befehl aus, um den TPM-Bezeichner zu erfassen. Stellen Sie sicher, dass Sie einen eindeutigen Namen für den Host angeben, der Sie bei der Suche nach HGS unterstützt. Sie benötigen diese Informationen, wenn Sie den Host außer Betrieb nehmen oder verhindern möchten, dass abgeschirmte VMs in HGS ausgeführt werden.

```
(Get-PlatformIdentifier -Name "Host01").InnerXml | Out-File C:\temp\host01.xml -Encoding UTF8
```

Kopieren Sie diese Datei auf Ihren HGS-Server, und führen Sie dann den folgenden Befehl aus, um den Host bei HGS zu registrieren.

```
Add-HgsAttestationTpmHost -Name 'Host01' -Path C:\temp\host01.xml
```

Hinzufügen einer neuen TPM-Baseline Wenn auf dem neuen Host eine neue Hardware-oder Firmwarekonfiguration für Ihre Umgebung ausgeführt wird, müssen Sie möglicherweise eine neue TPM-Baseline erstellen. Führen Sie hierzu den folgenden Befehl auf dem Host aus.

```
Get-HgsAttestationBaselinePolicy -Path 'C:\temp\hardwareConfig01.tcglog'
```

NOTE

Wenn Sie eine Fehlermeldung erhalten, die besagt, dass der Host die Überprüfung nicht erfolgreich war Dies ist eine Voraussetzungs Prüfung, um sicherzustellen, dass der Host abgeschirmte VMS ausführen kann. Dies bedeutet wahrscheinlich, dass Sie noch keine Code Integritätsrichtlinie oder andere erforderliche Einstellungen angewendet haben. Lesen Sie die Fehlermeldung, nehmen Sie die von ihr vorgeschlagenen Änderungen vor, und wiederholen Sie dann den Vorgang. Alternativ können Sie die Überprüfung zu diesem Zeitpunkt überspringen, indem Sie dem Befehl das `-SkipValidation` -Flag hinzufügen.

Kopieren Sie die TPM-Baseline auf Ihren HGS-Server, und registrieren Sie Sie mit dem folgenden Befehl. Wir empfehlen Ihnen, eine Benennungs Konvention zu verwenden, die Ihnen hilft, die Hardware-und Firmwarekonfiguration dieser Klasse von Hyper-V-Hosts zu verstehen.

```
Add-HgsAttestationTpmPolicy -Name 'HardwareConfig01' -Path 'C:\temp\hardwareConfig01.tcglog'
```

Hinzufügen einer neuen Code Integritätsrichtlinie Wenn Sie die Code Integritätsrichtlinie geändert haben, die auf Ihren Hyper-V-Hosts ausgeführt wird, müssen Sie die neue Richtlinie mit HGS registrieren, damit diese Hosts erfolgreich bestätigen können. Erfassen Sie auf einem Referenz Host, der als Master Abbild für die

vertrauenswürdigen Hyper-V-Computer in Ihrer Umgebung fungiert, mithilfe des Befehls `New-CIPolicy` eine neue CI-Richtlinie. Wir empfehlen Ihnen, die `filepublisher` -Ebene und den `hashback` für Hyper-V-Host-CI-Richtlinien zu verwenden. Erstellen Sie zunächst eine CI-Richtlinie im Überwachungsmodus, um sicherzustellen, dass alles wie erwartet funktioniert. Nachdem Sie eine Beispiel Arbeitsauslastung im System überprüft haben, können Sie die Richtlinie erzwingen und die erzwungene Version in HGS kopieren. Eine umfassende Liste der Konfigurationsoptionen für die Code Integritätsrichtlinie finden Sie in der [Device Guard-Dokumentation](#).

```
# Capture a new CI policy with the FilePublisher primary level and Hash fallback and enable user mode code
integrity protections
New-CIPolicy -FilePath 'C:\temp\ws2016-hardware01-ci.xml' -Level FilePublisher -Fallback Hash -UserPEs

# Apply the CI policy to the system
ConvertFrom-CIPolicy -XmlFilePath 'C:\temp\ws2016-hardware01-ci.xml' -BinaryFilePath 'C:\temp\ws2016-
hardware01-ci.p7b'
Copy-Item 'C:\temp\ws2016-hardware01-ci.p7b' 'C:\Windows\System32\CodeIntegrity\SIPolicy.p7b'
Restart-Computer

# Check the event log for any untrusted binaries and update the policy if necessary
# Consult the Device Guard documentation for more details

# Change the policy to be in enforced mode
Set-RuleOption -FilePath 'C:\temp\ws2016-hardare01-ci.xml' -Option 3 -Delete

# Apply the enforced CI policy on the system
ConvertFrom-CIPolicy -XmlFilePath 'C:\temp\ws2016-hardware01-ci.xml' -BinaryFilePath 'C:\temp\ws2016-
hardware01-ci.p7b'
Copy-Item 'C:\temp\ws2016-hardware01-ci.p7b' 'C:\Windows\System32\CodeIntegrity\SIPolicy.p7b'
Restart-Computer
```

Nachdem Sie die Richtlinie erstellt, getestet und erzwungen haben, kopieren Sie die Binärdatei (. p7b) auf Ihren HGS-Server, und registrieren Sie die Richtlinie.

```
Add-HgsAttestationCiPolicy -Name 'WS2016-Hardware01' -Path 'C:\temp\ws2016-hardware01-ci.p7b'
```

Hinzufügen eines Verschlüsselungsschlüssels für den Speicher Abbild

Wenn die `HGS_nodumps` -Richtlinie deaktiviert ist und `HGS_dumpencryption` -Richtlinie aktiviert ist, dürfen geschützte Hosts Speicher Abbilder (einschließlich Absturz Abbilder) aktivieren, damit Sie aktiviert werden, solange diese Abbilder verschlüsselt werden. Geschützte Hosts bestehen nur dann, wenn Sie entweder Speicher Abbilder deaktiviert haben oder Sie mit einem Schlüssel verschlüsseln, der HGS bekannt ist. Standardmäßig werden keine dumpverschlüsselungen Schlüssel auf HGS konfiguriert.

Verwenden Sie das Cmdlet "`Add-HgsAttestationDumpPolicy`", um HGS den Hashwert Ihres dumpverschlüsselungs Schlüssels hinzuzufügen. Wenn Sie eine TPM-Baseline auf einem Hyper-V-Host erfassen, der mit der dumpverschlüsselung konfiguriert ist, wird der Hash in tcglog eingeschlossen und kann für das Cmdlet "

`Add-HgsAttestationDumpPolicy`" bereitgestellt werden.

```
Add-HgsAttestationDumpPolicy -Name 'DumpEncryptionKey01' -Path
'C:\temp\TpmBaselineWithDumpEncryptionKey.tcglog'
```

Alternativ können Sie die Zeichen folgen Darstellung des Hashs direkt für das Cmdlet bereitstellen.

```
Add-HgsAttestationDumpPolicy -Name 'DumpEncryptionKey02' -PublicKeyHash '<paste your hash here>'
```

Stellen Sie sicher, dass Sie jeden eindeutigen Verschlüsselungsschlüssel für die Verschlüsselung zu HGS hinzufügen, wenn Sie sich für die Verwendung verschiedener Schlüssel in Ihrem geschützten Fabric entscheiden.

Hosts, die Speicher Abbilder mit einem Schlüssel verschlüsseln, der HGS nicht bekannt ist, erhalten keinen Nachweis.

Weitere Informationen zum [Konfigurieren der dumpverschlüsselung auf Hosts finden Sie in der Hyper-V-Dokumentation](#).

Überprüfen, ob das System den Nachweis überschritten hat

Nachdem Sie die erforderlichen Informationen bei HGS registriert haben, sollten Sie überprüfen, ob der Host den Nachweis übergibt. Führen Sie auf dem neu hinzugefügten Hyper-V-Host `Set-HgsClientConfiguration` aus, und geben Sie die richtigen URLs für Ihren HGS-Cluster an. Diese URLs können abgerufen werden, indem `Get-HgsServer` auf einem beliebigen HGS-Knoten ausgeführt wird.

```
Set-HgsClientConfiguration -KeyProtectionServerUrl 'http://hgs.bastion.local/KeyProtection' -
AttestationServerUrl 'http://hgs.bastion.local/Attestation'
```

Wenn der resultierende Status nicht "ishostbewacht: true" angibt, müssen Sie die Problembehandlung für die Konfiguration durchführen. Führen Sie auf dem Host, bei dem ein Fehler aufgetreten ist, den folgenden Befehl aus, um einen ausführlichen Bericht zu Problemen zu erhalten, die Ihnen helfen können, den fehlgeschlagenen Nachweis zu beheben.

```
Get-HgsTrace -RunDiagnostics -Detailed
```

IMPORTANT

Wenn Sie Windows Server 2019 oder Windows 10, Version 1809, verwenden und Code Integritäts Richtlinien verwenden, wird `Get-HgsTrace` möglicherweise einen Fehler für die aktive Diagnose der **Code Integritätsrichtlinie** zurückgeben. Sie können dieses Ergebnis gefahrlos ignorieren, wenn es die einzige Fehlerdiagnose ist.

Nachweis Richtlinien prüfen

Um den aktuellen Status der auf HGS konfigurierten Richtlinien zu überprüfen, führen Sie die folgenden Befehle auf einem beliebigen HGS-Knoten aus:

```
# List all trusted security groups for admin-trusted attestation
Get-HgsAttestationHostGroup

# List all policies configured for TPM-trusted attestation
Get-HgsAttestationPolicy
```

Wenn Sie feststellen, dass eine aktivierte Richtlinie nicht mehr Ihren Sicherheitsanforderungen entspricht (z. B. eine alte Code Integritätsrichtlinie, die jetzt als unsicher eingestuft wird), können Sie diese deaktivieren, indem Sie den Namen der Richtlinie im folgenden Befehl ersetzen:

```
Disable-HgsAttestationPolicy -Name 'PolicyName'
```

Auf ähnliche Weise können Sie `Enable-HgsAttestationPolicy` verwenden, um eine Richtlinie erneut zu aktivieren.

Wenn Sie eine Richtlinie nicht mehr benötigen und Sie von allen HGS-Knoten entfernen möchten, führen Sie `Remove-HgsAttestationPolicy -Name 'PolicyName'` aus, um die Richtlinie dauerhaft zu löschen.

Ändern der Nachweis Modi

Wenn Sie Ihr überwacht Fabric mit einem vom Administrator vertrauenswürdigen Nachweis gestartet haben,

möchten Sie wahrscheinlich ein Upgrade auf den weitaus stärkeren TPM-Nachweis Modus durchführen, sobald Sie über genügend TPM 2,0-kompatible Hosts in Ihrer Umgebung verfügen. Wenn Sie bereit sind, zu wechseln, können Sie alle Nachweis Artefakte (CI-Richtlinien, TPM-Basis Linien und TPM-IDs) in HGS vorab laden, während Sie weiterhin HGS mit dem Administrator vertrauenswürdigen Nachweis ausführen. Befolgen Sie hierzu einfach die Anweisungen im Abschnitt [autorisierender neuer](#) überwachter Hosts.

Nachdem Sie alle Ihre Richtlinien zu HGS hinzugefügt haben, besteht der nächste Schritt darin, einen synthetischen Nachweis Versuch auf Ihren Hosts auszuführen, um zu überprüfen, ob Sie den Nachweis im TPM-Modus bestanden haben. Dies wirkt sich nicht auf den aktuellen Betriebsstatus von HGS aus. Die folgenden Befehle müssen auf einem Computer ausgeführt werden, der Zugriff auf alle Hosts in der Umgebung und mindestens einen HGS-Knoten hat. Wenn die Firewall oder andere Sicherheitsrichtlinien dies verhindern, können Sie diesen Schritt überspringen. Nach Möglichkeit empfiehlt es sich, den synthetischen Nachweis durchführen, um einen guten Hinweis darauf zu erhalten, ob das "Kippen" in den TPM-Modus Ausfallzeiten für Ihre virtuellen Computer verursacht.

```
# Get information for each host in your environment
$hostNames = 'host01.contoso.com', 'host02.contoso.com', 'host03.contoso.com'
$credential = Get-Credential -Message 'Enter a credential with admin privileges on each host'
$targets = @()
$hostNames | ForEach-Object { $targets += New-HgsTraceTarget -Credential $credential -Role GuardedHost -
HostName $_ }

$hgsCredential = Get-Credential -Message 'Enter an admin credential for HGS'
$targets += New-HgsTraceTarget -Credential $hgsCredential -Role HostGuardianService -HostName
'HGS01.bastion.local'

# Initiate the synthetic attestation attempt
Get-HgsTrace -RunDiagnostics -Target $targets -Diagnostic GuardedFabricTpmMode
```

Überprüfen Sie nach Abschluss der Diagnose die ausgegebenen Informationen, um zu ermitteln, ob bei einem der Hosts im TPM-Modus ein Fehler aufgetreten ist. Führen Sie die Diagnose erneut aus, bis Sie von jedem Host einen "Pass" erhalten, und wechseln Sie dann zum Ändern von HGS in den TPM-Modus.

Das **Ändern in den TPM-Modus** dauert nur eine Sekunde. Führen Sie den folgenden Befehl auf einem beliebigen HGS-Knoten aus, um den Nachweis Modus zu aktualisieren.

```
Set-HgsServer -TrustTpm
```

Wenn Probleme auftreten und Sie zurück in den Active Directory-Modus wechseln müssen, können Sie dazu

```
Set-HgsServer -TrustActiveDirectory
```

 ausführen.

Nachdem Sie bestätigt haben, dass alles wie erwartet funktioniert, sollten Sie alle vertrauenswürdigen Active Directory Host Gruppen aus HGS entfernen und die Vertrauensstellung zwischen den HGS-und Fabric-Domänen entfernen. Wenn Sie die Active Directory Vertrauensstellung aktiviert haben, riskieren Sie, dass jemand die Vertrauensstellung erneut aktiviert und die HGS in Active Directory Modus wechselt. Dadurch kann nicht vertrauenswürdiger Code auf den überwachten Hosts deaktiviert werden.

Schlüsselverwaltung

Die geschützte Fabric-Lösung verwendet mehrere öffentliche/private Schlüsselpaare zum Überprüfen der Integrität der verschiedenen Komponenten in der Lösung und zum Verschlüsseln von Mandanten Geheimnissen. Der Host-Überwachungsdienst ist mit mindestens zwei Zertifikaten (mit öffentlichen und privaten Schlüsseln) konfiguriert, die zum Signieren und Verschlüsseln der Schlüssel verwendet werden, die zum Starten von abgeschirmten VMS verwendet werden. Diese Schlüssel müssen sorgfältig verwaltet werden. Wenn der private Schlüssel von einem Angreifer abgerufen wird, kann er alle virtuellen Computer, die in Ihrem Fabric ausgeführt werden, aufheben oder einen dort stunden-HGS-Cluster einrichten, der schwächere Nachweis Richtlinien

verwendet, um die von Ihnen eingerichteten Schutzmaßnahmen zu umgehen. Wenn Sie die privaten Schlüssel während eines Notfalls verlieren und nicht in einer Sicherung finden, müssen Sie ein neues Schlüsselpaar einrichten und jeden virtuellen Computer neu anordnen, um die neuen Zertifikate zu autorisieren.

In diesem Abschnitt werden die allgemeinen Schlüssel Verwaltungs Themen behandelt, mit denen Sie Ihre Schlüssel so konfigurieren können, dass Sie funktionsfähig und sicher sind.

Neue Schlüssel werden hinzugefügt

Obwohl HGS mit einem Satz von Schlüsseln initialisiert werden müssen, können Sie den HGS mehrere Verschlüsselungs- und Signatur Schlüssel hinzufügen. Die zwei häufigsten Gründe dafür, dass Sie HGS neue Schlüssel hinzufügen würden:

1. Zur Unterstützung von "Bring-your-own-Key"-Szenarien, in denen Mandanten Ihre privaten Schlüssel in das Hardware Sicherheitsmodul kopieren und nur Ihre Schlüssel zum Starten Ihrer abgeschirmten VMS autorisieren.
2. Um die vorhandenen Schlüssel für HGS zu ersetzen, indem Sie zuerst die neuen Schlüssel hinzufügen und beide Sätze von Schlüsseln aufbewahren, bis jede VM-Konfiguration aktualisiert wurde, um die neuen Schlüssel zu verwenden.

Der Vorgang zum Hinzufügen der neuen Schlüssel unterscheidet sich je nach Art des verwendeten Zertifikats.

Option 1: Hinzufügen eines in einem HSM gespeicherten Zertifikats

Die empfohlene Vorgehensweise zum Sichern von HGS-Schlüsseln ist die Verwendung von Zertifikaten, die in einem Hardware Sicherheitsmodul (HSM) erstellt werden. Mithilfe von HSMs wird sichergestellt, dass die Verwendung Ihrer Schlüssel an den physischen Zugriff auf ein Sicherheits sensibles Gerät in Ihrem Daten Center gebunden ist. Jedes HSM ist unterschiedlich und verfügt über einen eindeutigen Prozess zum Erstellen von Zertifikaten und Registrieren der Zertifikate bei HGS. Die folgenden Schritte sind für eine grobe Anleitung zur Verwendung von HSM-gestützten Zertifikaten vorgesehen. Die genauen Schritte und Funktionen finden Sie in der Dokumentation des HSM-Herstellers.

1. Installieren Sie die HSM-Software auf jedem HGS-Knoten in Ihrem Cluster. Abhängig davon, ob Sie über ein Netzwerk oder ein lokales HSM-Gerät verfügen, müssen Sie möglicherweise das HSM so konfigurieren, dass Ihr Computer Zugriff auf den Schlüsselspeicher erhält.
2. Erstellen von 2 Zertifikaten im HSM mit **2048-Bit-RSA-Schlüsseln** für die Verschlüsselung und Signierung
 - a. Erstellen Sie ein Verschlüsselungs Zertifikat mit der Schlüssel Verwendungs Eigenschaft "**Data Encipherment**" in Ihrem HSM.
 - b. Erstellen eines Signatur Zertifikats mit der Eigenschaft "Nutzung **digitaler Signatur** Schlüssel" in Ihrem HSM
3. Installieren Sie die Zertifikate im lokalen Zertifikat Speicher der einzelnen HGS-Knoten gemäß der Anleitung Ihres HSM-Herstellers.
4. Wenn Ihr HSM differenzierte Berechtigungen verwendet, um bestimmten Anwendungen oder Benutzern die Berechtigung zum Verwenden des privaten Schlüssels zu erteilen, müssen Sie Ihrem HGS-Gruppen verwalteten Dienst Konto Zugriff auf das Zertifikat gewähren. Sie können den Namen des HGS-GMSA-Kontos ermitteln, indem Sie ausführen `(Get-IISAppPool -Name KeyProtection).ProcessModel.UserName`
5. Fügen Sie die Signatur- und Verschlüsselungs Zertifikate zu HGS hinzu, indem Sie die Fingerabdrücke durch die der Zertifikate "in den folgenden Befehlen ersetzen:

```
Add-HgsKeyProtectionCertificate -CertificateType Encryption -Thumbprint
"AABBCCDDEEFF00112233445566778899"
Add-HgsKeyProtectionCertificate -CertificateType Signing -Thumbprint "99887766554433221100FFEEDDCCBBAA"
```

Option 2: Hinzufügen nicht exportierbarer Software-Zertifikate

Wenn Sie über ein Software-gestütztes Zertifikat verfügen, das von Ihrem Unternehmen oder von einer öffentlichen Zertifizierungsstelle ausgestellt wurde, die über einen nicht exportierbaren privaten Schlüssel verfügt, müssen Sie das Zertifikat mithilfe des Fingerabdrucks zu HGS hinzufügen.

1. Installieren Sie das Zertifikat auf Ihrem Computer gemäß den Anweisungen Ihrer Zertifizierungsstelle.
2. Erteilen Sie dem verwalteten Dienstkonto der HGS-Gruppe Lesezugriff auf den privaten Schlüssel des Zertifikats. Sie können den Namen des HGS-GMSA-Kontos ermitteln, indem Sie ausführen
(Get-IISAppPool -Name KeyProtection).ProcessModel.UserName
3. Registrieren Sie das Zertifikat mit dem folgenden Befehl bei HGS, und ersetzen Sie dabei den Fingerabdruck Ihres Zertifikats (Ändern der *Verschlüsselung* in *Signieren* für Signatur-Zertifikate):

```
Add-HgsKeyProtectionCertificate -CertificateType Encryption -Thumbprint
"AABBCCDDEEFF00112233445566778899"
```

IMPORTANT

Sie müssen den privaten Schlüssel manuell installieren und auf jedem HGS-Knoten Lesezugriff auf das GMSA-Konto gewähren. HGS können private Schlüssel für *ein* Zertifikat, das durch seinen Fingerabdruck registriert wird, nicht automatisch replizieren.

Option 3: Hinzufügen von in PFX-Dateien gespeicherten Zertifikaten

Wenn Sie über ein Software-gestütztes Zertifikat mit einem exportierbaren privaten Schlüssel verfügen, der im PFX-Dateiformat gespeichert und mit einem Kennwort gesichert werden kann, können die Zertifikate von HGS automatisch für Sie verwaltet werden. Zertifikate, die mit PFX-Dateien hinzugefügt werden, werden automatisch an jeden Knoten Ihres HGS-Clusters repliziert, und HGS sichert den Zugriff auf die privaten Schlüssel. Wenn Sie ein neues Zertifikat mit einer PFX-Datei hinzufügen möchten, führen Sie die folgenden Befehle auf einem beliebigen HGS-Knoten aus (ändern Sie die *Verschlüsselung* in *Signatur* für Signatur-Zertifikate):

```
$certPassword = Read-Host -AsSecureString -Prompt "Provide the PFX file password"
Add-HgsKeyProtectionCertificate -CertificateType Encryption -CertificatePath "C:\temp\encryptionCert.pfx" -
CertificatePassword $certPassword
```

Identifizieren und Ändern der primären Zertifikate Obwohl HGS mehrere Signatur- und Verschlüsselungs-Zertifikate unterstützen kann, wird ein paar als "primäre" Zertifikate verwendet. Dabei handelt es sich um die Zertifikate, die verwendet werden, wenn jemand die Wächter-Metadaten für diesen HGS-Cluster herunterlädt. Führen Sie den folgenden Befehl aus, um zu überprüfen, welche Zertifikate derzeit als primäre Zertifikate gekennzeichnet sind:

```
Get-HgsKeyProtectionCertificate -IsPrimary $true
```

Um ein neues primäres Verschlüsselungs- oder Signaturzertifikat festzulegen, suchen Sie den Fingerabdruck des gewünschten Zertifikats, und markieren Sie ihn mit den folgenden Befehlen als Primärschlüssel:

```
Get-HgsKeyProtectionCertificate
Set-HgsKeyProtectionCertificate -CertificateType Encryption -Thumbprint "AABBCCDDEEFF00112233445566778899" -
IsPrimary
Set-HgsKeyProtectionCertificate -CertificateType Signing -Thumbprint "99887766554433221100FFEEDDCCBBAA" -
IsPrimary
```

Erneuern oder Ersetzen von Schlüsseln

Wenn Sie die von HGS verwendeten Zertifikate erstellen, wird den Zertifikaten gemäß der Richtlinie Ihrer Zertifizierungsstelle und Ihren Anforderungs Informationen ein Ablaufdatum zugewiesen. Normalerweise müssen Zertifikate in Szenarien, in denen die Gültigkeit des Zertifikats wichtig ist, z. b. das Sichern von http-Kommunikationen, erneuert werden, bevor Sie ablaufen, um eine Dienst Unterbrechung oder eine Fehlermeldung zu vermeiden. HGS verwendet in diesem Sinne keine Zertifikate. HGS verwendet Zertifikate einfach als bequeme Möglichkeit zum Erstellen und Speichern eines asymmetrischen Schlüssel Paares. Ein abgelaufenes Verschlüsselungs-oder Signaturzertifikat auf HGS weist nicht auf eine Schwachstelle oder den Schutz von geschützten VMS hin. Außerdem werden Zertifikat Sperr Überprüfungen nicht von HGS ausgeführt. Wenn ein HGS-Zertifikat oder das Zertifikat der ausstellenden Zertifizierungsstelle widerrufen wird, hat dies keine Auswirkung auf die Verwendung des Zertifikats durch die HGS.

Sie müssen sich nur über ein HGS-Zertifikat Gedanken machen, wenn Sie der Meinung sind, dass der private Schlüssel gestohlen wurde. In diesem Fall besteht die Gefahr, dass die Integrität ihrer abgeschirmten VMS gefährdet ist, weil der Besitz der privaten Hälfte des HGS-Verschlüsselungs-und Signatur Schlüssel Paares ausreicht, um den Schutz auf einem virtuellen Computer zu entfernen oder einen gefälschten HGS-Server zu erhalten, der schwächere Nachweis Richtlinien aufweist.

Wenn Sie sich in dieser Situation befinden oder von Kompatibilitäts Standards zum regelmäßigen Aktualisieren von Zertifikat Schlüsseln benötigt werden, wird in den folgenden Schritten der Prozess zum Ändern der Schlüssel auf einem HGS-Server beschrieben. Beachten Sie, dass die folgende Anleitung ein bedeutendes Unternehmen darstellt, das zu einer Dienst Unterbrechung für jede VM führt, die vom HGS-Cluster bedient wird. Die richtige Planung für das Ändern von HGS-Schlüsseln ist erforderlich, um die Dienst Unterbrechung zu minimieren und die Sicherheit von Mandanten-VMS

Führen Sie auf einem HGS-Knoten die folgenden Schritte aus, um ein neues Paar von Verschlüsselungs-und Signatur Zertifikaten zu registrieren. Ausführliche Informationen zu den verschiedenen Möglichkeiten zum Hinzufügen neuer Schlüssel zu HGS finden Sie im Abschnitt zum Hinzufügen [neuer Schlüssel](#) .

1. Erstellen Sie ein neues Paar von Verschlüsselungs-und Signatur Zertifikaten für Ihren HGS-Server. Im Idealfall werden diese in einem Hardware Sicherheitsmodul erstellt.
2. Registrieren der neuen Verschlüsselungs-und Signatur Zertifikate mit **Add-hgskeyscertificate**

```
Add-HgsKeyProtectionCertificate -CertificateType Signing -Thumbprint <Thumbprint>
Add-HgsKeyProtectionCertificate -CertificateType Encryption -Thumbprint <Thumbprint>
```

3. Wenn Sie Fingerabdrücke verwendet haben, müssen Sie zu jedem Knoten im Cluster wechseln, um den privaten Schlüssel zu installieren und dem HGS-GMSA Zugriff auf den Schlüssel zu gewähren.
4. Erstellen der neuen Zertifikate als Standardzertifikate in HGS

```
Set-HgsKeyProtectionCertificate -CertificateType Signing -Thumbprint <Thumbprint> -IsPrimary
Set-HgsKeyProtectionCertificate -CertificateType Encryption -Thumbprint <Thumbprint> -IsPrimary
```

An diesem Punkt werden geschützte Daten, die mit Metadaten aus dem HGS-Knoten erstellt werden, die neuen Zertifikate verwenden, vorhandene virtuelle Computer funktionieren jedoch weiterhin, da die älteren Zertifikate weiterhin vorhanden sind. Um sicherzustellen, dass alle vorhandenen VMS mit den neuen Schlüsseln

funktionieren, müssen Sie die Schlüssel Schutzvorrichtung auf den einzelnen virtuellen Computern aktualisieren. Dabei handelt es sich um eine Aktion, die erfordert, dass der Besitzer des virtuellen Computers (Person oder Entität, die den "Owner"-Wächter besitzt) beteiligt ist. Führen Sie für jede abgeschirmte VM die folgenden Schritte aus: 5. Fahren Sie den virtuellen Computer herunter. Der virtuelle Computer kann erst wieder eingeschaltet werden, wenn die restlichen Schritte ausgeführt wurden. andernfalls müssen Sie den Prozess erneut starten. 6. Aktuelle Schlüssel Schutzvorrichtung in einer Datei speichern:

```
Get-VMKeyProtector -VMName 'VM001' | Out-File '.\VM001.kp'
```

7. Übertragen der KP in den VM-Besitzer 8. Lassen Sie den Besitzer die aktualisierten Überwachungsinformationen von HGS herunterladen und auf Ihrem lokalen System importieren 9. Lesen Sie die aktuelle KP in den Arbeitsspeicher, gewähren Sie dem neuen Erziehungsberechtigten Zugriff auf die KP, und speichern Sie Sie in einer neuen Datei, indem Sie die folgenden Befehle ausführen:

```
```powershell
$kpraw = Get-Content -Path .\VM001.kp
$kp = ConvertTo-HgsKeyProtector -Bytes $kpraw
$newGuardian = Get-HgsGuardian -Name 'UpdatedHgsGuardian'
$updatedKP = Grant-HgsKeyProtectorAccess -KeyProtector $kp -Guardian $newGuardian
$updatedKP.RawData | Out-File .\updatedVM001.kp
```
```

10. Kopieren Sie die aktualisierte KP zurück in das hostingfabric.

11. Wenden Sie die KP auf den ursprünglichen virtuellen Computer an:

```
$updatedKP = Get-Content -Path .\updatedVM001.kp
Set-VMKeyProtector -VMName VM001 -KeyProtector $updatedKP
```

12. Starten Sie die VM, und stellen Sie sicher, dass Sie erfolgreich ausgeführt wird.

NOTE

Wenn der VM-Besitzer eine falsche Schlüssel Schutzvorrichtung auf dem virtuellen Computer festlegt und Ihr Fabric nicht zum Ausführen des virtuellen Computers autorisiert, können Sie den abgeschirmten virtuellen Computer nicht starten. Um zur letzten als funktionierend bekannten Schlüssel Schutzvorrichtung zurückzukehren, führen Sie

```
Set-VMKeyProtector -RestoreLastKnownGoodKeyProtector
```

Nachdem alle VMs aktualisiert wurden, um die neuen Wächter Schlüssel zu autorisieren, können Sie die alten Schlüssel deaktivieren und entfernen.

13. Holen Sie sich die Fingerabdrücke der alten Zertifikate aus

```
Get-HgsKeyProtectionCertificate -IsPrimary $false
```

14. Deaktivieren Sie die einzelnen Zertifikate, indem Sie die folgenden Befehle ausführen:

```
Set-HgsKeyProtectionCertificate -CertificateType Signing -Thumbprint <Thumbprint> -IsEnabled $false
Set-HgsKeyProtectionCertificate -CertificateType Encryption -Thumbprint <Thumbprint> -IsEnabled $false
```

15. Nachdem Sie sichergestellt haben, dass die VMs weiterhin mit deaktivierten Zertifikaten gestartet werden können, entfernen Sie die Zertifikate aus HGS, indem Sie die folgenden Befehle ausführen:

```
Remove-HgsKeyProtectionCertificate -CertificateType Signing -Thumbprint <Thumbprint>`
Remove-HgsKeyProtectionCertificate -CertificateType Encryption -Thumbprint <Thumbprint>`
```

IMPORTANT

VM-Sicherungen enthalten alte schlüsselschutzinformationen, mit denen die alten Zertifikate zum Starten der VM verwendet werden können. Wenn Sie wissen, dass Ihr privater Schlüssel kompromittiert wurde, sollten Sie davon ausgehen, dass die VM-Sicherungen ebenfalls kompromittiert werden können, und die entsprechenden Maßnahmen ergreifen. Durch das Zerstören der VM-Konfiguration aus den Sicherungen (vmcx-Dateien) werden die Schlüssel Schutzvorrichtungen entfernt. Dies führt dazu, dass das BitLocker-Wiederherstellungs Kennwort zum nächsten Mal zum Starten der VM verwendet werden muss.

Schlüssel Replikation zwischen Knoten

Jeder Knoten im HGS-Cluster muss mit denselben Verschlüsselungs-, Signatur- und (wenn konfigurierten) SSL-Zertifikaten konfiguriert werden. Dies ist erforderlich, um sicherzustellen, dass die Anforderungen von Hyper-V-Hosts, die zu einem beliebigen Knoten im Cluster gelangen, erfolgreich bedient werden können.

Wenn Sie den HGS-Server mit PFX-basierten Zertifikaten initialisiert haben, repliziert HGS automatisch sowohl den öffentlichen als auch den privaten Schlüssel dieser Zertifikate auf allen Knoten im Cluster. Sie müssen nur die Schlüssel auf einem Knoten hinzufügen.

Wenn Sie den HGS-Server mit Zertifikat verweisen oder Fingerabdrücken initialisiert haben, repliziert HGS den *öffentlichen* Schlüssel im Zertifikat nur auf jeden Knoten. Darüber hinaus kann HGS selbst keinen Zugriff auf den privaten Schlüssel auf einem Knoten in diesem Szenario gewähren. Daher sind Sie für folgende Aufgaben verantwortlich:

1. Installieren Sie den privaten Schlüssel auf jedem HGS-Knoten.
2. Gewähren Sie dem Gruppen verwalteten Dienst Konto (Managed Service Account, GMSA) der HGS-Gruppe Zugriff auf den privaten Schlüssel auf jedem Knoten, da diese Aufgaben zusätzliche Betriebsbelastung erfordern, sind Sie jedoch für HSM-gestützte Schlüssel und Zertifikate mit nicht exportierbaren privaten Schlüsseln erforderlich.

SSL-Zertifikate werden nie in irgendeiner Form repliziert. Es liegt in ihrer Verantwortung, jeden HGS-Server mit demselben SSL-Zertifikat zu initialisieren und jeden Server zu aktualisieren, wenn Sie das SSL-Zertifikat erneuern oder ersetzen. Wenn Sie das SSL-Zertifikat ersetzen, empfiehlt es sich, das Cmdlet [Set-hgsserver](#) zu verwenden.

Aufheben der Konfiguration von HGS

Wenn Sie einen HGS-Server außer Betrieb setzen oder erheblich neu konfigurieren müssen, können Sie dazu die Cmdlets [Clear-hgsserver](#) oder [Uninstall-hgsserver](#) verwenden.

Löschen der HGS-Konfiguration

Verwenden Sie zum Entfernen eines Knotens aus dem HGS-Cluster das Cmdlet [Clear-hgsserver](#). Mit diesem Cmdlet werden auf dem Server, auf dem es ausgeführt wird, die folgenden Änderungen vorgenommen:

- Hebt die Registrierung der Nachweis- und Schlüsselschutz Dienste auf.
- Entfernt den Jea-Verwaltungs Endpunkt "Microsoft. Windows. HGS".
- Entfernt den lokalen Computer aus dem HGS-Failovercluster.

Wenn der Server der letzte HGS-Knoten im Cluster ist, werden auch der Cluster und die zugehörige verteilte Netzwerknamen Ressource zerstört.

```
# Removes the local computer from the HGS cluster
Clear-HgsServer
```

Nachdem der Löschvorgang abgeschlossen ist, kann der HGS-Server mit [Initialize-hgsserver](#) erneut initialisiert werden. Wenn Sie [install-hgsserver](#) zum Einrichten einer Active Directory Domain Services Domäne verwendet

haben, bleibt diese Domäne nach dem Löschvorgang konfiguriert und betriebsbereit.

Deinstallieren von HGS

Wenn Sie einen Knoten aus dem HGS-Cluster entfernen **und** den Active Directory-Domäne Controller herabstufen möchten, auf dem er ausgeführt wird, verwenden Sie das Cmdlet [Uninstall-hgsserver](#). Mit diesem Cmdlet werden auf dem Server, auf dem es ausgeführt wird, die folgenden Änderungen vorgenommen:

- Hebt die Registrierung der Nachweis- und Schlüsselschutz Dienste auf.
- Entfernt den Jea-Verwaltungs Endpunkt "Microsoft. Windows. HGS".
- Entfernt den lokalen Computer aus dem HGS-Failovercluster.
- Herabstufen des Active Directory-Domäne Controllers, sofern konfiguriert

Wenn es sich bei dem Server um den letzten HGS-Knoten im Cluster handelt, werden die Domäne, der Failovercluster und die verteilte Netzwerknamen Ressource des Clusters ebenfalls zerstört.

```
# Removes the local computer from the HGS cluster and demotes the ADDC (restart required)
$newLocalAdminPassword = Read-Host -AsSecureString -Prompt "Enter a new password for the local administrator account"
Uninstall-HgsServer -LocalAdministratorPassword $newLocalAdminPassword -Restart
```

Nachdem der Deinstallations Vorgang abgeschlossen und der Computer neu gestartet wurde, können Sie addc und HGS mithilfe von [install-hgsserver](#) neu installieren oder den Computer einer Domäne hinzufügen und den HGS-Server in dieser Domäne mit [initialisieren-hgsserver](#) initialisieren.

Wenn Sie den Computer nicht mehr als HGS-Knoten verwenden möchten, können Sie die Rolle aus Windows entfernen.

```
Uninstall-WindowsFeature HostGuardianServiceRole
```

Überlegungen zu Filialen

09.04.2020 • 6 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal),

Dieser Artikel beschreibt bewährte Methoden für die Ausführung von abgeschirmten virtuellen Computern in Zweigniederlassungen und in anderen Remote Szenarien, in denen Hyper-V-Hosts Zeiträume mit eingeschränkter Konnektivität zu HGS aufweisen können.

Fall Back Konfiguration

Ab Windows Server, Version 1709, können Sie einen zusätzlichen Satz von Host-Überwachungsdienst-URLs auf Hyper-V-Hosts konfigurieren, die verwendet werden, wenn Ihre primäre HGS nicht reagiert. Auf diese Weise können Sie einen lokalen HGS-Cluster ausführen, der als primärer Server verwendet wird, um eine bessere Leistung zu erzielen. Sie können dann auf die HGS Ihres Unternehmens Rechenzentrums zurückgreifen, wenn die lokalen Server ausfallen.

Wenn Sie die Fall Back-Option verwenden möchten, müssen Sie zwei HGS-Server einrichten. Sie können Windows Server 2019 oder Windows Server 2016 ausführen und sind entweder Teil desselben oder unterschiedlichen Clusters. Wenn es sich um verschiedene Cluster handelt, sollten Sie operative Verfahren einrichten, um sicherzustellen, dass die Nachweis Richtlinien zwischen den beiden Servern synchronisiert werden. Beide müssen in der Lage sein, den Hyper-V-Host ordnungsgemäß zu autorisieren, um abgeschirmte VMS auszuführen, und Sie müssen über das Schlüsselmaterail verfügen, das zum Starten der abgeschirmten VMS Sie können entweder ein paar frei gegebener Verschlüsselungs- und Signatur Zertifikate zwischen den beiden Clustern verwenden oder separate Zertifikate verwenden und die abgeschirmte HGS-VM so konfigurieren, dass beide Wächter (Verschlüsselungs-/Signatur-zertifikatpaare) in der Schutz Datendatei autorisiert werden.

Aktualisieren Sie dann Ihre Hyper-V-Hosts auf Windows Server-Version 1709 oder Windows Server 2019, und führen Sie den folgenden Befehl aus:

```
# Replace https://hgs.primary.com and https://hgs.backup.com with your own domain names and protocols
Set-HgsClientConfiguration -KeyProtectionServerUrl 'https://hgs.primary.com/KeyProtection' -
AttestationServerUrl 'https://hgs.primary.com/Attestation' -FallbackKeyProtectionServerUrl
'https://hgs.backup.com/KeyProtection' -FallbackAttestationServerUrl 'https://hgs.backup.com/Attestation'
```

Wenn Sie die Konfiguration eines Fall Back Servers aufheben möchten, lassen Sie einfach beide Fall back Parameter aus:

```
Set-HgsClientConfiguration -KeyProtectionServerUrl 'https://hgs.primary.com/KeyProtection' -
AttestationServerUrl 'https://hgs.primary.com/Attestation'
```

Damit der Hyper-V-Host den Nachweis sowohl mit dem primären als auch dem Fall Back Server übergibt, müssen Sie sicherstellen, dass Ihre Nachweis Informationen mit beiden HGS-Clustern auf dem neuesten Stand sind. Außerdem müssen die Zertifikate, mit denen das TPM des virtuellen Computers entschlüsselt wird, in beiden HGS-Clustern verfügbar sein. Sie können jeden HGS mit verschiedenen Zertifikaten konfigurieren und den virtuellen Computer so konfigurieren, dass er sowohl vertrauenswürdig ist, als auch einen freigegebenen Satz von Zertifikaten zu beiden HGS-Clustern hinzufügen.

Weitere Informationen zum Konfigurieren von HGS in einer Zweigstelle mithilfe von Fall Back-URLs finden Sie im Blogbeitrag [verbesserte Unterstützung für Zweigstellen für abgeschirmte VMs in Windows Server, Version 1709](#).

Offline Modus

Im Offline Modus kann die abgeschirmte VM aktiviert werden, wenn HGS nicht erreicht werden kann, solange die Sicherheitskonfiguration des Hyper-V-Hosts nicht geändert wurde. Der Offline Modus funktioniert, indem eine spezielle Version der TPM-Schlüssel Schutzvorrichtung des virtuellen Computers auf dem Hyper-V-Host zwischengespeichert wird. Die Schlüssel Schutzvorrichtung wird in die aktuelle Sicherheitskonfiguration des Hosts (mit dem virtualisierungsbasierten Sicherheits Identitätsschlüssel) verschlüsselt. Wenn der Host nicht mit HGS kommunizieren kann und seine Sicherheitskonfiguration nicht geändert wurde, kann er die zwischengespeicherte Schlüssel Schutzvorrichtung zum Starten der abgeschirmten VM verwenden. Wenn sich die Sicherheitseinstellungen auf dem System ändern, z. b. eine neue Code Integritätsrichtlinie, die angewendet wird, oder der sichere Start deaktiviert wird, werden die zwischengespeicherten Schlüssel Schutzvorrichtungen für ungültig erklärt, und der Host muss einen HGS bestätigen, damit alle abgeschirmten VMS erneut offline gestartet werden können.

Der Offline Modus erfordert Windows Server Insider Preview Build 17609 oder höher sowohl für den Host-Überwachungsdienst Cluster als auch für den Hyper-V-Host. Sie wird durch eine Richtlinie auf HGS gesteuert, die standardmäßig deaktiviert ist. Um die Unterstützung für den Offline Modus zu aktivieren, führen Sie den folgenden Befehl auf einem HGS-Knoten aus:

```
Set-HgsKeyProtectionConfiguration -AllowKeyMaterialCaching:$true
```

Da die zwischen speicherbaren Schlüssel Schutzvorrichtungen für jeden abgeschirmten virtuellen Computer eindeutig sind, müssen Sie den vollständigen Herunterfahren (kein Neustart) durchlaufen und die abgeschirmten VMs starten, um eine zwischen speicherbare Schlüssel Schutzvorrichtung zu erhalten, nachdem diese Einstellung auf HGS aktiviert wurde. Wenn Ihre abgeschirmte VM zu einem Hyper-V-Host migriert wird, auf dem eine ältere Version von Windows Server ausgeführt wird, oder eine neue Schlüssel Schutzvorrichtung aus einer älteren Version von HGS erhält, kann Sie nicht im Offline Modus gestartet werden, Sie kann jedoch weiterhin im Online Modus ausgeführt werden, wenn der Zugriff auf HGS verfügbar ist.

Upgrade eines überwachten Fabric auf Windows Server 2019

09.04.2020 • 11 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

In diesem Artikel werden die Schritte beschrieben, die erforderlich sind, um ein vorhandenes geschütztes Fabric von Windows Server 2016, Windows Server Version 1709 oder Windows Server Version 1803 auf Windows Server 2019 zu aktualisieren.

Neuerungen in Windows Server 2019

Wenn Sie ein überwachtes Fabric unter Windows Server 2019 ausführen, können Sie mehrere neue Features nutzen:

Der **Host Schlüssel** Nachweis ist unser neuester Nachweis Modus, der so konzipiert ist, dass abgeschirmte VMS leichter ausgeführt werden können, wenn Ihre Hyper-V-Hosts nicht über TPM 2,0-Geräte verfügen, die für den TPM-Nachweis verfügbar sind. Der Host Schlüssel Nachweis verwendet Schlüsselpaare zum Authentifizieren von Hosts mit HGS, sodass Hosts nicht mit einer Active Directory Domäne verknüpft werden müssen, wodurch die AD-Vertrauensstellung zwischen HGS und der Unternehmens Gesamtstruktur entfällt und die Anzahl der geöffneten Firewallports reduziert wird. Der Host Schlüssel Nachweis ersetzt Active Directory Nachweis, der in Windows Server 2019 als veraltet markiert ist.

V2 -Nachweis Version: zur Unterstützung von Host Schlüssel Nachweis und neuen Features in Zukunft haben wir die Versionierung in HGS eingeführt. Eine Neuinstallation von HGS unter Windows Server 2019 führt dazu, dass der Server einen v2-Nachweis durchführt. Dies bedeutet, dass der Host Schlüssel Nachweis für Windows Server 2019-Hosts unterstützt wird und noch v1-Hosts unter Windows Server 2016 unterstützt werden. Direkte Upgrades auf 2019 verbleiben bei Version v1, bis Sie v2 manuell aktivieren. Die meisten Cmdlets verfügen jetzt über den Parameter "-hgsversion", mit dem Sie angeben können, ob Sie mit Legacy-oder modernen Nachweis Richtlinien arbeiten möchten.

Unterstützung für abgeschirmte Linux-VMs : Hyper-V-Hosts unter Windows Server 2019 können abgeschirmte Linux-VMs ausführen. Während sich seit Windows Server, Version 1709, abgeschirmte VMS von Linux befinden, ist Windows Server 2019 die erste langfristige Wartung der Kanal Version, um Sie zu unterstützen.

Verbesserungen bei Filialen : Wir haben das Ausführen von abgeschirmten VMs in Zweigstellen mit Unterstützung für abgeschirmte Offline-VMS und Fall Back Konfigurationen auf Hyper-V-Hosts vereinfacht.

TPM-Host Bindung : für die sichersten Workloads, bei denen eine abgeschirmte VM nur auf dem ersten Host ausgeführt werden soll, auf dem Sie erstellt wurde, können Sie die VM nun mithilfe des TPM des Hosts an diesen Host binden. Dies eignet sich am besten für Arbeitsstationen mit privilegiertem Zugriff und nicht für allgemeine Rechenzentrums Workloads, die zwischen Hosts migriert werden müssen.

Kompatibilitätsmatrix

Bevor Sie das geschützte Fabric auf Windows Server 2019 aktualisieren, sollten Sie die folgende Kompatibilitäts Matrix überprüfen, um festzustellen, ob Ihre Konfiguration unterstützt wird.

| | WS2016-HGS | WS2019-HGS |
|---------------------|--------------------------------|--------------------------|
| WS2016 Hyper-V-Host | Unterstützt | Unterstützt ¹ |
| WS2019 Hyper-V-Host | Nicht unterstützt ² | Unterstützt |

¹ Windows Server 2016-Hosts können nur Windows Server 2019 HGS-Server mithilfe des v1-Nachweis Protokolls belegen. Neue Features, die exklusiv im v2-Nachweis Protokoll verfügbar sind, einschließlich des Host Schlüssel Nachweis, werden für Windows Server 2016-Hosts nicht unterstützt.

² Microsoft kennt ein Problem, das verhindert, dass Windows Server 2019-Hosts, die den TPM-Nachweis verwenden, erfolgreich auf einem Windows Server 2016 HGS-Server getestet werden. Diese Einschränkung wird in einem zukünftigen Update für Windows Server 2016 behoben werden.

Aktualisieren von HGS auf Windows Server 2019

Es wird empfohlen, das Upgrade Ihres HGS-Clusters auf Windows Server 2019 durchzuführen, bevor Sie ein Upgrade für Ihre Hyper-V-Hosts durchführen, um sicherzustellen, dass alle Hosts, ob Sie Windows Server 2016 oder 2019 ausführen, erfolgreich bestätigt werden können.

Wenn Sie Ihren HGS-Cluster aktualisieren, müssen Sie einen Knoten temporär aus dem Cluster entfernen, während er aktualisiert wird. Dadurch wird die Kapazität Ihres Clusters reduziert, um auf Anforderungen von Ihren Hyper-V-Hosts zu reagieren. Dies kann zu langsamen Reaktionszeiten oder Dienst Ausfällen für Ihre Mandanten führen. Stellen Sie sicher, dass Sie über genügend Kapazität verfügen, um Ihre Nachweis- und schlüsselfreigabe Anforderungen zu verarbeiten, bevor Sie ein Upgrade für einen HGS

Um Ihr HGS-Cluster zu aktualisieren, führen Sie die folgenden Schritte auf jedem Knoten des Clusters, jeweils jeweils einem Knoten aus:

1. Entfernen Sie den HGS-Server aus Ihrem Cluster durch Ausführen von `Clear-HgsServer` an einer PowerShell-Eingabeaufforderung mit erhöhten Rechten. Mit diesem Cmdlet werden der replizierte HGS-Speicher, die HGS-Websites und der Knoten aus dem Failovercluster entfernt.
2. Wenn es sich bei dem HGS-Server um einen Domänen Controller (Standardkonfiguration) handelt, müssen Sie `adprep /forestprep` ausführen und `adprep /domainprep` auf dem ersten Knoten ausführen, der aktualisiert wird, um die Domäne für ein Betriebssystem Upgrade vorzubereiten. Weitere Informationen finden Sie in der [Active Directory Domain Services Upgradedokumentation](#).
3. Führen Sie ein direktes Upgrade auf Windows Server 2019 [aus](#).
4. Führen Sie [Initialize-hgsserver](#) aus, um den Knoten wieder zum Cluster hinzuzufügen.

Nachdem alle Knoten auf Windows Server 2019 aktualisiert wurden, können Sie optional die HGS-Version auf v2 aktualisieren, um neue Features wie den Host Schlüssel Nachweis zu unterstützen.

```
Set-HgsServerVersion v2
```

Aktualisieren von Hyper-V-Hosts auf Windows Server 2019

Bevor Sie ein Upgrade für Ihre Hyper-v-Hosts auf Windows Server 2019 durchführen, stellen Sie sicher, dass Ihr HGS-Cluster bereits auf Windows Server 2019 aktualisiert wurde und Sie alle virtuellen Computer vom Hyper-v-Server verschoben haben.

1. Wenn Sie Windows Defender-Anwendungs Steuerungs Code-Integritäts Richtlinien auf dem Server verwenden (immer bei der Verwendung des TPM-Nachweis), stellen Sie sicher, dass die Richtlinie entweder im Überwachungsmodus oder deaktiviert ist, bevor Sie versuchen, den Server zu aktualisieren. [Erfahren Sie, wie](#)

[Sie eine WDac-Richtlinie deaktivieren](#)

2. Befolgen Sie die Anweisungen im [Windows Server-upgradeinhalt](#), um Ihren Host auf Windows Server 2019 zu aktualisieren. Wenn Ihr Hyper-V-Host Teil eines Failoverclusters ist, können Sie ein paralleles [Upgrade des Cluster Betriebssystems](#) in Erwägung gezogen.
3. Testen Sie Ihre Windows Defender-Anwendungs Steuerungs Richtlinie, [und aktivieren](#) Sie Sie erneut, wenn Sie vor dem Upgrade eine aktiviert haben.
4. Führen Sie `Get-HgsClientConfiguration` aus, um zu überprüfen, ob `ishostbewacht = true` ist. Dies bedeutet, dass der Host erfolgreich mit Ihrem HGS-Server übergeben wird.
5. Wenn Sie einen TPM-Nachweis verwenden, müssen Sie [die TPM-Baseline oder die Code Integritätsrichtlinie](#) nach dem Upgrade erneut erfassen, um den Nachweis zu erfüllen.
6. Erneutes Ausführen von abgeschirmten VMS auf dem Host

Zum Host Schlüssel Nachweis wechseln

Führen Sie die folgenden Schritte aus, wenn Sie zurzeit Active Directory basierten Nachweis ausführen und ein Upgrade auf den Host Schlüssel Nachweis durchführen möchten. Beachten Sie, dass der Active Directory basierte Nachweis in Windows Server 2019 veraltet ist und in einer zukünftigen Version möglicherweise entfernt wird.

1. Stellen Sie sicher, dass der HGS-Server im v2-Nachweis Modus betrieben wird, indem Sie den folgenden Befehl ausführen. Vorhandene v1-Hosts werden auch dann weiterhin überzeugen, wenn der HGS-Server auf v2 aktualisiert wird.

```
Set-HgsServerVersion v2
```

2. [Generieren Sie Host Schlüssel](#) von jedem ihrer Hyper-V-Hosts, und registrieren Sie Sie bei HGS. Da sich HGS weiterhin im Active Directory Modus befindet, wird eine Warnung angezeigt, dass die neuen Host Schlüssel nicht sofort wirksam werden. Dies ist beabsichtigt, da Sie nicht in den Host Schlüssel Modus wechseln möchten, bis alle Hosts erfolgreich mit Host Schlüsseln bestätigt werden.
3. Nachdem die Host Schlüssel für jeden Host registriert wurden, können Sie HGS so konfigurieren, dass der Host Schlüssel Nachweis Modus verwendet wird:

```
Set-HgsServer -TrustHostKey
```

Wenn Sie Probleme mit dem Host Schlüssel Modus haben und auf Active Directory basierten Nachweis zurückkehren müssen, führen Sie den folgenden Befehl auf HGS aus:

```
Set-HgsServer -TrustActiveDirectory
```

Problembehandlung bei einem geschützten Fabric

09.04.2020 • 2 minutes to read • [Edit Online](#)

In den folgenden Themen wird das Behandeln von Problemen mit einem geschützten Fabric behandelt:

- [Problembehandlung mithilfe des geschützten Fabric-Diagnosetools](#)
- [Problembehandlung beim Host-Überwachungsdienst](#)
- [Problembehandlung für geschützte Hosts](#)
- [Problembehandlung bei geschützten VMS](#)

Siehe auch

- [Bereitstellen des Host-Überwachungs Diensts für geschützte Hosts und abgeschirmte VMS](#)
- [Verwalten eines geschützten Fabrics](#)

Problembehandlung mithilfe des geschützten Fabric-Diagnosetools

09.04.2020 • 27 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

In diesem Thema wird beschrieben, wie Sie häufige Fehler bei der Bereitstellung, Konfiguration und beim laufenden Betrieb der geschützten Fabric-Infrastruktur mithilfe des geschützten Fabric-Diagnosetools identifizieren und beheben. Dies schließt den Host-Überwachungsdienst (Host Guardian Service, HGS), alle überwachten Hosts und unterstützende Dienste wie DNS und Active Directory ein. Das Diagnosetool kann verwendet werden, um einen ersten Durchlauf bei der Selektierung eines fehlerhaften geschützten Fabric durchzuführen, sodass Administratoren einen Ausgangspunkt für die Behebung von Ausfällen und die Identifizierung falsch konfigurierter Assets erhalten. Das Tool ist kein Ersatz für einen fundierten Einblick in das Betreiben eines geschützten Fabric und dient nur der schnellen Überprüfung der häufigsten Probleme, die bei alltäglichen Vorgängen auftreten.

Eine vollständige Dokumentation der in diesem Artikel verwendeten Cmdlets finden Sie in der [Referenz zum hgstdiagnostics-Modul](#).

NOTE

Beim Ausführen des Diagnosetools für geschützte Fabric (Get-HgsTrace - RunDiagnostics), kann es zu der falschen Statusangabe führen, dass die HTTPS-Konfiguration fehlerhaft ist, obwohl sie nicht unterbrochen oder nicht verwendet wird. Dieser Fehler kann unabhängig vom Nachweis Modus der HGS zurückgegeben werden. Es gibt zahlreiche mögliche Ursachen:

- HTTPS ist tatsächlich nicht ordnungsgemäß konfiguriert/beschädigt
- Sie verwenden einen Administrator vertrauenswürdigen Nachweis, und die Vertrauensstellung ist beschädigt.
 - Dies ist unabhängig davon, ob HTTPS ordnungsgemäß konfiguriert, nicht ordnungsgemäß oder gar nicht verwendet wird.

Beachten Sie, dass die Diagnose nur einen falschen Status zurückgibt, wenn das Ziel ein Hyper-V-Host ist. Wenn das Ziel der Diagnose der Host Guardian Dienst ist, ist der zurückgegebene Status korrekt.

Schnellstart

Sie können entweder einen überwachten Host oder einen HGS-Knoten diagnostizieren, indem Sie den folgenden Befehl in einer Windows PowerShell-Sitzung mit lokalen Administratorrechten aufrufen:

```
Get-HgsTrace -RunDiagnostics -Detailed
```

Dadurch wird automatisch die Rolle des aktuellen Hosts erkannt und relevante Probleme, die automatisch erkannt werden können, diagnostiziert. Alle Ergebnisse, die während dieses Vorgangs generiert werden, werden angezeigt, da der `-Detailed`-Schalter vorhanden ist.

Im restlichen Teil dieses Themas finden Sie eine ausführliche Exemplarische Vorgehensweise für die Erweiterte Verwendung von `Get-HgsTrace` zum Ausführen von Aufgaben wie der gleichzeitigen Diagnose mehrerer Hosts und zum erkennen komplexer Knoten übergreifender Fehlkonfigurationen.

Diagnose Übersicht

Die geschützte Fabric-Diagnose ist auf jedem Host verfügbar, auf dem geschützte virtuelle computerbezogene Tools und Features installiert sind, einschließlich Hosts, auf denen Server Core ausgeführt wird. Derzeit sind die Diagnosen in den folgenden Features/Paketen enthalten:

1. Rolle "Host-Überwachungsdienst"
2. Host-Überwachungsunterstützung für Hyper-V
3. VM-Abschirmungstools für Fabric-Verwaltung
4. Remoteserver-Verwaltungstools (RSAT)

Dies bedeutet, dass Diagnosetools auf allen überwachten Hosts, HGS-Knoten, bestimmten Fabric-Verwaltungs Servern und allen Windows 10-Arbeitsstationen verfügbar sind, auf denen **rsat** installiert ist. Die Diagnose kann von einem der oben genannten Computer aus aufgerufen werden, um alle überwachten Hosts oder HGS-Knoten in einem geschützten Fabric zu diagnostizieren. mithilfe von remotelaufverfolgungs-Zielen kann die Diagnose andere Hosts als den Computer mit Diagnose suchen und verbinden.

Jeder Host, der als Ziel der Diagnose dient, wird als "Ablauf Verfolgungs Ziel" bezeichnet. Ablauf Verfolgungs Ziele werden anhand ihrer Hostnamen und Rollen identifiziert. Rollen beschreiben die Funktion, die ein bestimmtes Ablauf Verfolgungs Ziel in einem geschützten Fabric ausführt. Derzeit unterstützen Ablauf Verfolgungs Ziele **HostGuardianService** -und **GuardedHost** Rollen. Beachten Sie, dass es möglich ist, dass ein Host mehrere Rollen gleichzeitig einnimmt und auch von der Diagnose unterstützt wird. Dies sollte jedoch nicht in Produktionsumgebungen erfolgen. Die HGS-und Hyper-V-Hosts sollten stets getrennt und voneinander getrennt werden.

Administratoren können alle Diagnose Tasks starten, indem Sie **Get-HgsTrace** ausführen. Dieser Befehl führt zwei unterschiedliche Funktionen basierend auf den Schaltern aus, die zur Laufzeit bereitgestellt werden: Ablauf Verfolgungs Sammlung und-Diagnose. Diese beiden kombinierten bilden das gesamte geschützte Fabric-Diagnose Tool. Obwohl Sie nicht explizit erforderlich sind, erfordern die meisten nützlichen Diagnosen Ablauf Verfolgungen, die nur mit Administrator Anmelde Informationen für das Ziel der Ablauf Verfolgung erfasst werden können. Wenn der Benutzer, der die Ablauf Verfolgungs Sammlung ausführt, unzureichende Berechtigungen erhält, schlagen Ablauf Verfolgungen fehl, die eine Rechte Erweiterung erfordern, während alle anderen bestanden werden. Dies ermöglicht eine partielle Diagnose in dem Fall, dass ein unterprivilegierter Operator eine selektiert durchführt.

Ablauf Verfolgungs Sammlung

Standardmäßig werden von **Get-HgsTrace** nur Ablauf Verfolgungen erfasst und in einem temporären Ordner gespeichert. Ablauf Verfolgungen haben das Format eines Ordners, der nach dem Zielhost benannt ist und mit speziell formatierten Dateien gefüllt ist, die beschreiben, wie der Host konfiguriert ist. Die Ablauf Verfolgungen enthalten außerdem Metadaten, die beschreiben, wie die Diagnose zum Erfassen der Ablauf Verfolgungen aufgerufen wurde. Diese Daten werden von der Diagnose verwendet, um beim Ausführen der manuellen Diagnoseinformationen über den Host zu reaktivieren.

Bei Bedarf können Ablauf Verfolgungen manuell überprüft werden. Alle Formate sind entweder von Menschen lesbar (XML) oder können mithilfe von Standard Tools (z. b. x. 509-Zertifikaten und den Windows-Crypto Shell-Erweiterungen) problemlos überprüft werden. Beachten Sie jedoch, dass Ablauf Verfolgungen nicht für die manuelle Diagnose konzipiert sind und es immer effektiver ist, die Ablauf Verfolgungen mit den Diagnosefunktionen von **Get-HgsTrace** zu verarbeiten.

Die Ergebnisse der Ausführung der Ablauf Verfolgungs Sammlung geben keine Anzeichen für die Integrität eines bestimmten Hosts an. Sie geben einfach an, dass Ablauf Verfolgungen erfolgreich erfasst wurden. Es ist erforderlich, die Diagnosefunktionen von **Get-HgsTrace** zu verwenden, um zu bestimmen, ob die Ablauf Verfolgungen auf eine fehlerhafte Umgebung hindeuten.

Mithilfe des **-Diagnostic** -Parameters können Sie die Ablauf Verfolgungs Sammlung auf die Ablauf Verfolgungen beschränken, die für den Betrieb der angegebenen Diagnose erforderlich sind. Dadurch wird die Menge der

erfassten Daten sowie die zum Aufrufen der Diagnose erforderlichen Berechtigungen reduziert.

Diagnose

Erfasste Ablauf Verfolgungen können von bereitgestellten `Get-HgsTrace` den Speicherort der Ablauf Verfolgungen über den Parameter `-Path` und durch Angabe des `-RunDiagnostics` Schalters diagnostiziert werden. Außerdem können `Get-HgsTrace` die Erfassung und Diagnose in einem einzigen Durchlauf durchführen, indem Sie den `-RunDiagnostics` -Schalter und eine Liste von Ablauf Verfolgungs Zielen bereitstellen. Wenn keine Ablauf Verfolgungs Ziele bereitgestellt werden, wird der aktuelle Computer als implizites Ziel verwendet, dessen Rolle durch die Überprüfung der installierten Windows PowerShell-Module abgeleitet ist.

Die Diagnose führt zu einem hierarchischen Format, das anzeigt, welche Ablauf Verfolgungs Ziele, Diagnose Sätze und die einzelnen Diagnosen für einen bestimmten Fehler verantwortlich sind. Zu den Fehlern zählen Empfehlungen zur Wiederherstellung und Behebung, wenn eine Entscheidung getroffen werden kann, welche Aktion als nächstes ausgeführt werden soll. Standardmäßig werden das übergeben und das irrelevante Ergebnis ausgeblendet. Wenn Sie alle von der Diagnose getesteten Elemente anzeigen möchten, geben Sie den `-Detailed` Switch an. Dies bewirkt, dass alle Ergebnisse unabhängig von Ihrem Status angezeigt werden.

Es ist möglich, den Satz der Diagnose, die mithilfe des `-Diagnostic` -Parameters ausgeführt werden, einzuschränken. Dadurch können Sie angeben, welche Klassen der Diagnose für die Ablauf Verfolgungs Ziele ausgeführt werden sollen, und alle anderen unterdrücken. Beispiele für verfügbare Diagnoseklassen sind Netzwerk, bewährte Methoden und Client Hardware. In der [Cmdlet-Dokumentation](#) finden Sie eine aktuelle Liste der verfügbaren Diagnosen.

WARNING

Die Diagnose ist kein Ersatz für eine sichere Pipeline zur Überwachung und Reaktion auf Vorfälle. Es gibt ein System Center Operations Manager Paket für die Überwachung überwachter Fabrics sowie verschiedene Ereignisprotokoll Kanäle, die überwacht werden können, um Probleme frühzeitig zu erkennen. Die Diagnose kann dann verwendet werden, um diese Fehler schnell zu selektiert und eine Vorgehensweise festzulegen.

Ziel Diagnose

`Get-HgsTrace` für Ablauf Verfolgungs Ziele. Ein Ablauf Verfolgungs Ziel ist ein Objekt, das einem HGS-Knoten oder einem überwachten Host in einem geschützten Fabric entspricht. Dies kann als Erweiterung einer `PSSession` betrachtet werden, die nur die Informationen enthält, die nur von der Diagnose (z. b. der Rolle des Hosts im Fabric) benötigt werden. Ziele können implizit (z. b. lokale oder manuelle Diagnose) oder explizit mit dem `New-HgsTraceTarget` Befehl generiert werden.

Lokale Diagnose

Standardmäßig wird für `Get-HgsTrace` der localhost (d. h., wo das Cmdlet aufgerufen wird) als Ziel verwendet. Dies wird als implizites lokales Ziel bezeichnet. Das implizite lokale Ziel wird nur verwendet, wenn im `-Target` -Parameter keine Ziele bereitgestellt werden und im `-Path` keine bereits vorhandenen Ablauf Verfolgungen gefunden werden.

Das implizite lokale Ziel verwendet einen Rollen Rückschluss, um zu bestimmen, welche Rolle der aktuelle Host im geschützten Fabric spielt. Dies basiert auf den installierten Windows PowerShell-Modulen, die ungefähr den Funktionen entsprechen, die auf dem System installiert wurden. Das Vorhandensein des `HgsServer` Moduls bewirkt, dass das Ablauf Verfolgungs Ziel die Rolle übernimmt `HostGuardianService` und das Vorhandensein des Moduls `HgsClient` bewirkt, dass das Ablauf Verfolgungs Ziel die Rolle `GuardedHost` übernimmt. Es ist möglich, dass für einen bestimmten Host beide Module vorhanden sind. In diesem Fall wird er sowohl als `HostGuardianService` als auch als `GuardedHost` behandelt.

Daher ist der Standard Aufruf der Diagnose für die lokale Erfassung von Ablauf Verfolgungen:

```
Get-HgsTrace
```

... entspricht Folgendem:

```
New-HgsTraceTarget -Local | Get-HgsTrace
```

TIP

`Get-HgsTrace` können Ziele über die Pipeline oder direkt über den Parameter `-Target` akzeptieren. Es gibt keinen Unterschied zwischen den beiden operationalen.

Remote Diagnose mithilfe von Ablauf Verfolgungs Zielen

Es ist möglich, einen Host Remote zu diagnostizieren, indem er Ablauf Verfolgungs Ziele mit Remote Verbindungsinformationen erzeugt. Alles, was erforderlich ist, ist der Hostname und ein Satz von Anmelde Informationen, die mithilfe von Windows PowerShell-Remoting eine Verbindung herstellen können.

```
$server = New-HgsTraceTarget -HostName "hgs-01.secure.contoso.com" -Role HostGuardianService -Credential  
(Enter-Credential)  
Get-HgsTrace -RunDiagnostics -Target $server
```

In diesem Beispiel wird eine Aufforderung zum Erfassen der Anmelde Informationen des Remote Benutzers generiert. Anschließend wird die Diagnose mithilfe des Remote Hosts auf `hgs-01.secure.contoso.com` ausgeführt, um die Ablauf Verfolgungs Sammlung abzuschließen. Die resultierenden Ablauf Verfolgungen werden auf den localhost heruntergeladen und anschließend diagnostiziert. Die Diagnoseergebnisse werden genauso wie bei der [lokalen Diagnose](#) angezeigt. Ebenso ist es nicht notwendig, eine Rolle anzugeben, da Sie auf Grundlage der auf dem Remote System installierten Windows PowerShell-Module abgeleitet werden kann.

Bei der Remote Diagnose werden Windows PowerShell-Remoting für alle Zugriffe auf den Remote Host verwendet. Daher ist es eine Voraussetzung dafür, dass für das Ablauf Verfolgungs Ziel Windows PowerShell-Remoting aktiviert ist (siehe [Aktivieren von psremoting](#)) und dass der localhost ordnungsgemäß für das Starten von Verbindungen mit dem Ziel konfiguriert ist.

NOTE

In den meisten Fällen ist es lediglich erforderlich, dass "localhost" ein Teil derselben Active Directory Gesamtstruktur ist und dass ein gültiger DNS-Hostname verwendet wird. Wenn Ihre Umgebung ein komplizierteres Verbund Modell verwendet oder Sie direkte IP-Adressen für die Konnektivität verwenden möchten, müssen Sie möglicherweise eine zusätzliche Konfiguration durchführen, z. b. das Festlegen von WinRM- [vertrauenswürdigen Hosts](#).

Sie können überprüfen, ob ein Ablauf Verfolgungs Ziel ordnungsgemäß instanziiert und für das akzeptieren von Verbindungen konfiguriert ist, indem Sie das `Test-HgsTraceTarget` Cmdlet verwenden:

```
$server = New-HgsTraceTarget -HostName "hgs-01.secure.contoso.com" -Role HostGuardianService -Credential  
(Enter-Credential)  
$server | Test-HgsTraceTarget
```

Dieser Befehl gibt `$True` nur dann zurück, wenn `Get-HgsTrace` eine Remote Diagnose Sitzung mit dem Ablauf Verfolgungs Ziel einrichten könnte. Bei einem Fehler gibt dieses Cmdlet relevante Statusinformationen zur weiteren Problembehandlung der Windows PowerShell-Remoting-Verbindung zurück.

Implizite Anmelde Informationen

Wenn eine Remote Diagnose von einem Benutzer mit ausreichenden Berechtigungen zum Herstellen einer Remote Verbindung mit dem Ablauf Verfolgungs Ziel durchgeführt wird, ist es nicht erforderlich, Anmelde Informationen für die `New-HgsTraceTarget` bereitzustellen. Das Cmdlet "`Get-HgsTrace`" verwendet automatisch die Anmelde Informationen des Benutzers, der das Cmdlet aufgerufen hat, wenn er eine Verbindung öffnet.

WARNING

Einige Einschränkungen gelten für die Wiederverwendung von Anmelde Informationen, insbesondere bei der Durchführung eines "zweiten Hops". Dies tritt auf, wenn versucht wird, Anmelde Informationen aus einer Remote Sitzung auf einem anderen Computer wiederzuverwenden. [CredSSP](#) muss zur Unterstützung dieses Szenarios eingerichtet werden, aber dies liegt außerhalb des Umfangs der Verwaltung und Problembehandlung für geschützte Fabrics.

Verwenden von Windows PowerShell Just Enough Administration (Jea) und Diagnostics

Die Remote Diagnose unterstützt die Verwendung von mit Jea eingeschränkten Windows PowerShell-Endpunkten. Standardmäßig werden Remote Ablauf Verfolgungs Ziele mithilfe des Standard-`microsoft.powershell` Endpunkts verbunden. Wenn das Ziel der Ablauf Verfolgung über die `HostGuardianService` Rolle verfügt, wird auch versucht, den `microsoft.windows.hgs` Endpunkt zu verwenden, der bei der Installation von HGS konfiguriert wird.

Wenn Sie einen benutzerdefinierten Endpunkt verwenden möchten, müssen Sie den Namen der Sitzungs Konfiguration angeben, während Sie das Ziel der Ablauf Verfolgung mit dem `-PSSessionConfigurationName` Parameter erstellen, z. b. unten:

```
New-HgsTraceTarget -HostName "hgs-01.secure.contoso.com" -Role HostGuardianService -Credential (Enter-Credential) -PSSessionConfigurationName "microsoft.windows.hgs"
```

Diagnostizieren mehrerer Hosts

Sie können mehrere Ablauf Verfolgungs Ziele gleichzeitig an `Get-HgsTrace` übergeben. Dies schließt eine Mischung aus lokalen und Remote Zielen ein. Jedes Ziel wird ihrerseits verfolgt, und dann werden die Ablauf Verfolgungen von jedem Ziel gleichzeitig diagnostiziert. Das Diagnosetool kann die erweiterten Kenntnisse der Bereitstellung nutzen, um komplexe Knoten übergreifende Fehlkonfigurationen zu identifizieren, die sonst nicht erkennbar sind. Die Verwendung dieser Funktion erfordert nur die gleichzeitige Bereitstellung von Ablauf Verfolgungen mehrerer Hosts (bei manueller Diagnose) oder das Festlegen mehrerer Hosts beim Aufrufen von `Get-HgsTrace` (im Fall einer Remote Diagnose).

Hier finden Sie ein Beispiel für die Verwendung der Remote Diagnose zum selektiert eines Fabrics aus zwei HGS-Knoten und zwei überwachten Hosts, bei denen einer der überwachten Hosts verwendet wird, um `Get-HgsTrace` zu starten.

```
$hgs01 = New-HgsTraceTarget -HostName "hgs-01.secure.contoso.com" -Credential (Enter-Credential)
$hgs02 = New-HgsTraceTarget -HostName "hgs-02.secure.contoso.com" -Credential (Enter-Credential)
$gh01 = New-HgsTraceTarget -Local
$gh02 = New-HgsTraceTarget -HostName "guardedhost-02.contoso.com"
Get-HgsTrace -Target $hgs01,$hgs02,$gh01,$gh02 -RunDiagnostics
```

NOTE

Bei der Diagnose mehrerer Knoten ist es nicht erforderlich, das gesamte geschützte Fabric zu diagnostizieren. In vielen Fällen genügt es, alle Knoten einzuschließen, die möglicherweise an einer bestimmten Fehlerbedingung beteiligt sind. Dabei handelt es sich normalerweise um eine Teilmenge der überwachten Hosts und eine bestimmte Anzahl von Knoten aus dem HGS-Cluster.

Manuelle Diagnose mit gespeicherten Ablauf Verfolgungen

Manchmal möchten Sie die Diagnose erneut ausführen, ohne die Ablauf Verfolgungen erneut zu erfassen, oder Sie verfügen möglicherweise nicht über die erforderlichen Anmelde Informationen, um alle Hosts in Ihrem Fabric gleichzeitig Remote zu diagnostizieren. Bei der manuellen Diagnose handelt es sich um einen Mechanismus, mit dem Sie mithilfe von `Get-HgsTrace` weiterhin eine gesamte fabricrouterlung ausführen können, ohne eine Remote Ablauf Verfolgungs Sammlung zu verwenden.

Vor der manuellen Diagnose müssen Sie sicherstellen, dass die Administratoren jedes Hosts im Fabric, das als veraltet gilt, bereit sind und bereit sind, Befehle in Ihrem Namen auszuführen. Bei der Ausgabe der Diagnose Ablauf Verfolgung werden keine Informationen verfügbar gemacht, die im Allgemeinen als vertraulich angesehen werden. Allerdings ist es für den Benutzer von nutzen, um festzustellen, ob diese Informationen sicher für andere Personen verfügbar gemacht werden können

NOTE

Ablauf Verfolgungen werden nicht anonymisiert und zeigen Netzwerkconfiguration, PKI-Einstellungen und andere Konfigurationen, die manchmal als private Informationen angesehen werden. Daher sollten Ablauf Verfolgungen nur an vertrauenswürdige Entitäten innerhalb einer Organisation übertragen und nie öffentlich veröffentlicht werden.

Die Schritte zum Ausführen einer manuellen Diagnose lauten wie folgt:

1. Fordern Sie an, dass die einzelnen Host Administratoren `Get-HgsTrace` die Angabe eines bekannten `-Path` und die Liste der Diagnose, die Sie für die resultierenden Ablauf Verfolgungen ausführen möchten, ausführen. Beispiel:

```
Get-HgsTrace -Path C:\Traces -Diagnostic Networking,BestPractices
```

2. Fordern Sie an, dass die einzelnen Host Administratoren den resultierenden Ablauf Verfolgungs Ordner Verpacken und an Sie senden. Dieser Prozess kann über e-Mail, über Dateifreigaben oder einen anderen Mechanismus gesteuert werden, basierend auf den Betriebsrichtlinien und Verfahren, die von Ihrer Organisation festgelegt wurden.
3. Alle empfangenen Ablauf Verfolgungen ohne anderen Inhalt oder Ordner in einem einzelnen Ordner zusammenführen.
 - Nehmen Sie beispielsweise an, dass Ihre Administratoren Ihnen die von den vier Computern erfassten Ablauf Verfolgungen mit den Namen HGS-01, HGS-02, RR1N2608-12 und RR1N2608-13 senden. Jeder Administrator hätte Ihnen einen Ordner mit demselben Namen gesendet. Sie würden eine Verzeichnisstruktur zusammenstellen, die wie folgt aussieht:

```
FabricTraces
|- HGS-01
|  |- TargetMetadata.xml
|  |- Metadata.xml
|  |- [any other trace files for this host]
|- HGS-02
|  |- [...]
|- RR1N2608-12
|  |- [...]
|- RR1N2608-13
|  |- [...]
```

4. Führen Sie die Diagnose aus, und geben Sie den Pfad zum assemblierten Ablauf Verfolgungs Ordner für den `-Path`-Parameter an, und geben Sie den `-RunDiagnostics`-Switch sowie die Diagnoseinformationen an, für die Sie Ihre Administratoren aufgefordert haben, Die Diagnose geht davon aus, dass Sie nicht auf die im Pfad gefundenen Hosts zugreifen kann und versucht daher, nur die vorab erfassten Ablauf Verfolgungen

zu verwenden. Wenn Ablauf Verfolgungen fehlen oder beschädigt sind, tritt bei der Diagnose nur ein Fehler auf, und der Vorgang wird normal fortgesetzt. Beispiel:

```
Get-HgsTrace -RunDiagnostics -Diagnostic Networking,BestPractices -Path ".\FabricTraces"
```

Mischung gespeicherter Ablauf Verfolgungen mit zusätzlichen Zielen

In einigen Fällen verfügen Sie möglicherweise über eine Reihe von vorab gesammelten Ablauf Verfolgungen, die Sie mit zusätzlichen Host Überwachungen erweitern möchten. Es ist möglich, vorab erfasste Ablauf Verfolgungen mit zusätzlichen Zielen zu kombinieren, die in einem einzigen Diagnose- und Diagnose Vorgang verfolgt werden.

Befolgen Sie die Anweisungen zum Erfassen und Zusammenstellen eines oben angegebenen Ablauf Verfolgungs Ordners, `Get-HgsTrace` mit zusätzlichen Ablauf Verfolgungs Zielen, die im vorab erfassten Ablauf Verfolgungs Ordner nicht gefunden werden:

```
$hgs03 = New-HgsTraceTarget -HostName "hgs-03.secure.contoso.com" -Credential (Enter-Credential)
Get-HgsTrace -RunDiagnostics -Target $hgs03 -Path .\FabricTraces
```

Das Diagnose-Cmdlet identifiziert alle vorab gesammelten Hosts und den einen zusätzlichen Host, der weiterhin verfolgt werden muss und die erforderliche Ablauf Verfolgung ausführt. Die Summe aller vorab gesammelten und frisch gesammelten Ablauf Verfolgungen wird dann diagnostiziert. Der resultierende Ablauf Verfolgungs Ordner enthält sowohl die alte als auch die neue Ablauf Verfolgung.

Bekannte Probleme

Bei der Ausführung unter Windows Server 2019 oder Windows 10, Version 1809 und neueren Betriebssystemversionen hat das Modul für geschützte Fabric-Diagnosen bekannte Einschränkungen. Die Verwendung der folgenden Funktionen kann zu fehlerhaften Ergebnissen führen:

- Host Schlüssel Nachweis
- Nur Nachweis-HGS-Konfiguration (für SQL Server Always Encrypted Szenarien)
- Verwendung von v1-Richtlinien Artefakten auf einem HGS-Server, bei dem der Standardwert der Nachweis Richtlinie "V2" lautet

Ein Fehler in `Get-HgsTrace` bei der Verwendung dieser Features weist nicht notwendigerweise darauf hin, dass der HGS-Server oder der geschützte Host falsch konfiguriert ist. Verwenden Sie andere Diagnosetools wie `Get-HgsClientConfiguration` auf einem überwachten Host, um zu testen, ob ein Host den Nachweis überschritten hat.

Problembehandlung beim Host-Überwachungsdienst

09.04.2020 • 16 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

In diesem Thema werden Lösungen für häufige Probleme beschrieben, die beim Bereitstellen oder betreiben eines HGS-Servers (Host Wächter Service) in einem geschützten Fabric auftreten. Wenn Sie sich nicht sicher sind, welche Art von Problem Sie haben, versuchen Sie zunächst, die [geschützte Fabric-Diagnose](#) auf Ihren HGS-Servern und Hyper-V-Hosts auszuführen, um die möglichen Gründe einzugrenzen.

Zertifikate

HGS erfordert für den Betrieb mehrere Zertifikate, einschließlich des vom Administrator konfigurierten Verschlüsselungs- und Signatur Zertifikats sowie eines von HGS selbstverwalteten Nachweis Zertifikats. Wenn diese Zertifikate nicht ordnungsgemäß konfiguriert sind, können von HGS keine Anforderungen von Hyper-V-Hosts bedient werden, die Schlüssel Schutzvorrichtungen für abgeschirmte VMS bestätigen oder entsperren möchten. In den folgenden Abschnitten werden allgemeine Probleme im Zusammenhang mit auf HGS konfigurierten Zertifikaten behandelt.

Zertifikat Berechtigungen

HGS müssen in der Lage sein, auf die öffentlichen und privaten Schlüssel der Verschlüsselungs- und Signatur Zertifikate zuzugreifen, die durch den Zertifikat Fingerabdruck zu HGS hinzugefügt werden. Insbesondere das Gruppen verwaltete Dienst Konto (Group Managed Service Account, GMSA), das den HGS-Dienst ausführt, benötigt Zugriff auf die Schlüssel. Führen Sie den folgenden Befehl in einer PowerShell-Eingabeaufforderung mit erhöhten Rechten auf Ihrem HGS-Server aus, um den von HGS verwendeten GMSA zu finden:

```
(Get-IISAppPool -Name KeyProtection).ProcessModel.UserName
```

Wie Sie dem GMSA-Konto den Zugriff auf den privaten Schlüssel gewähren, hängt davon ab, wo der Schlüssel gespeichert ist: auf dem Computer als lokale Zertifikat Datei, in einem Hardware Sicherheitsmodul (HSM) oder mithilfe eines benutzerdefinierten Schlüsselspeicher Anbieters von Drittanbietern.

Gewähren des Zugriffs auf softwaregestützte private Schlüssel

Wenn Sie ein selbst signiertes Zertifikat oder ein Zertifikat verwenden, das von einer Zertifizierungsstelle ausgestellt wurde, die **nicht** in einem Hardware Sicherheitsmodul oder einem benutzerdefinierten Schlüsselspeicher Anbieter gespeichert ist, können Sie die Berechtigungen für den privaten Schlüssel ändern, indem Sie die folgenden Schritte ausführen:

1. Öffnen Sie den lokalen Zertifikat-Manager (certlm. msc).
2. Erweitern Sie die Option **persönliche > Zertifikate** , und suchen Sie das Signatur- oder Verschlüsselungs Zertifikat, das Sie aktualisieren möchten.
3. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie **Alle Tasks > private Schlüssel verwalten**
4. Klicken Sie auf **Hinzufügen** , um einem neuen Benutzer Zugriff auf den privaten Schlüssel des Zertifikats zu gewähren.
5. Geben Sie in der Objektauswahl den Namen des GMSA-Kontos für die zuvor gefundenen HGS ein, und klicken Sie dann auf **OK**.
6. Stellen Sie sicher, dass GMSA über **Lese** Zugriff auf das Zertifikat verfügt.

7. Klicken Sie auf **OK** , um das Fenster Berechtigung zu schließen.

Wenn Sie HGS auf Server Core ausführen oder den Server remote verwalten, können Sie keine privaten Schlüssel mit dem lokalen Zertifikat-Manager verwalten. Stattdessen müssen Sie das [PowerShell-Modul für geschützte Fabric-Tools](#) herunterladen, mit dem Sie die Berechtigungen in PowerShell verwalten können.

1. Öffnen Sie eine PowerShell-Konsole mit erhöhten Rechten auf dem Server Core-Computer, oder verwenden Sie PowerShell-Remoting mit einem Konto, das über lokale Administrator Berechtigungen für HGS verfügt.
2. Führen Sie die folgenden Befehle aus, um das PowerShell-Modul für geschützte Fabric-Tools zu installieren und dem GMSA-Konto Zugriff auf den privaten Schlüssel zu gewähren.

```
$certificateThumbprint = '<ENTER CERTIFICATE THUMBPRINT HERE>'

# Install the Guarded Fabric Tools module, if necessary
Install-Module -Name GuardedFabricTools -Repository PSGallery

# Import the module into the current session
Import-Module -Name GuardedFabricTools

# Get the certificate object
$cert = Get-Item "Cert:\LocalMachine\My\$certificateThumbprint"

# Get the gMSA account name
$gMSA = (Get-IISAppPool -Name KeyProtection).ProcessModel.UserName

# Grant the gMSA read access to the certificate
$cert.Acl = $cert.Acl | Add-AccessRule $gMSA Read Allow
```

Gewähren des Zugriffs auf HSM oder benutzerdefinierte private Schlüssel des Anbieters

Wenn die privaten Schlüssel Ihres Zertifikats von einem Hardware Sicherheitsmodul (HSM) oder einem benutzerdefinierten Schlüsselspeicher Anbieter (KSP) unterstützt werden, hängt das Berechtigungs Modell von Ihrem spezifischen Softwareanbieter ab. Um die besten Ergebnisse zu erzielen, finden Sie auf der Dokumentation oder Support Website Ihres Herstellers Informationen dazu, wie die Berechtigungen für private Schlüssel für ihr bestimmtes Gerät bzw. Ihre Software behandelt werden. In jedem Fall benötigt das von HGS verwendete GMSA *Lesen* Berechtigungen für die privaten Schlüssel für die Verschlüsselung, Signatur und den Kommunikations Zertifikat, damit Signierungs-und Verschlüsselungs Vorgänge durchgeführt werden können.

Einige Hardware Sicherheitsmodule unterstützen nicht das Gewähren von Zugriff auf einen privaten Schlüssel für bestimmte Benutzerkonten. Stattdessen wird dem Computer Konto der Zugriff auf alle Schlüssel in einem bestimmten Schlüsselsatz gestattet. Bei solchen Geräten ist es in der Regel ausreichend, dem Computer den Zugriff auf Ihre Schlüssel zu gewähren, und HGS können diese Verbindung nutzen.

Tipps für HSMs

Unten sind die empfohlenen Konfigurationsoptionen aufgeführt, die Sie bei der erfolgreichen Verwendung von HSM-gestützten Schlüsseln mit HGS basierend auf den Erfahrungen von Microsoft und den zugehörigen Partnern unterstützen. Diese Tipps werden Ihnen zur Verfügung gestellt und sind nicht garantiert, dass Sie zum Zeitpunkt des Lesens korrekt sind. Sie werden auch nicht von den HSM-Herstellern unterstützt. Wenn Sie weitere Fragen haben, wenden Sie sich an Ihren HSM-Hersteller, um genaue Informationen zu Ihrem speziellen Gerät zu erhalten.

| | |
|---------------------|-----------|
| HSM - MARKE/- REIHE | VORSCHLAG |
|---------------------|-----------|

| HSM - MARKE/- REIHE | VORSCHLAG |
|----------------------|--|
| Gemalto SafeNet | Stellen Sie sicher, dass die Eigenschaft Schlüssel Verwendung in der Zertifikat Anforderungs Datei auf 0xa0 festgelegt ist, sodass das Zertifikat zum Signieren und Verschlüsseln verwendet werden kann. Außerdem müssen Sie dem GMSA-Konto mit dem lokalen Zertifikat-Manager-Tool <i>Lese</i> Zugriff auf den privaten Schlüssel gewähren (siehe die obigen Schritte). |
| "nCipher nShield" | Stellen Sie sicher, dass jeder HGS-Knoten Zugriff auf die Security World hat, die Signatur-und Verschlüsselungsschlüssel enthält. Außerdem müssen Sie ggf. den GMSA <i>Lese</i> Zugriff auf den privaten Schlüssel mit dem lokalen Zertifikat-Manager gewähren (siehe die obigen Schritte). |
| Utimaco-kryptoserver | Stellen Sie sicher, dass die Eigenschaft Schlüssel Verwendung in der Zertifikat Anforderungs Datei auf 0x13 festgelegt ist, sodass das Zertifikat für die Verschlüsselung, Entschlüsselung und Signierung verwendet werden kann. |

Zertifikat Anforderungen

Wenn Sie eine Zertifizierungsstelle zum Ausstellen Ihrer Zertifikate in einer Public Key-Infrastruktur (PKI)-Umgebung verwenden, müssen Sie sicherstellen, dass Ihre Zertifikat Anforderung die Mindestanforderungen für die Verwendung dieser Schlüssel durch die HGS enthält.

Signieren von Zertifikaten

| CSR-EIGENSCHAFT | ERFORDERLICHER WERT |
|---------------------|--------------------------------------|
| Algorithmus | RSA |
| Schlüsselgröße | Mindestens 2048 Bits |
| Schlüsselverwendung | Signatur/Vorzeichen/DigitalSignature |

Verschlüsselungs Zertifikate

| CSR-EIGENSCHAFT | ERFORDERLICHER WERT |
|---------------------|--|
| Algorithmus | RSA |
| Schlüsselgröße | Mindestens 2048 Bits |
| Schlüsselverwendung | Verschlüsselung/Verschlüsselung/DataEncipherment |

Vorlagen für Active Directory Zertifikat Dienste

Wenn Sie die Zertifikat Vorlagen für die Zertifikat Dienste (Active Directory Certificate Services, ADCS) zum Erstellen der Zertifikate verwenden, empfiehlt es sich, eine Vorlage mit den folgenden Einstellungen zu verwenden:

| ADCS-VORLAGEN EIGENSCHAFT | ERFORDERLICHER WERT |
|---------------------------|---------------------------|
| Anbieter Kategorie | Schlüsselspeicheranbieter |

| ADCS-VORLAGEN EIGENSCHAFT | ERFORDERLICHER WERT |
|-----------------------------------|---|
| Algorithmusname | RSA |
| Minimale Schlüsselgröße | 2.048 |
| Zweck | Signatur und Verschlüsselung |
| Schlüssel Verwendungs Erweiterung | Digitale Signatur, Schlüssel Verschlüsselung, Datenverschlüsselung ("Verschlüsselung von Benutzerdaten zulassen") |

Zeit Abweichung

Wenn die Zeit Ihres Servers maßgeblich von der von anderen HGS-Knoten oder Hyper-V-Hosts in Ihrem geschützten Fabric abweicht, treten möglicherweise Probleme mit der Gültigkeit des Nachweis Zertifikats des Nachweis Vorgangs auf. Das Signatur Geber Zertifikat wird im Hintergrund auf HGS erstellt und erneuert und zum Signieren von Integritäts Zertifikaten verwendet, die vom Nachweis Dienst für überwachte Hosts ausgestellt wurden.

Führen Sie den folgenden Befehl an einer PowerShell-Eingabeaufforderung mit erhöhten Rechten aus, um das Signatur Geber Zertifikat zu aktualisieren.

```
Start-ScheduledTask -TaskPath \Microsoft\Windows\HGSServer -TaskName
AttestationSignerCertRenewalTask
```

Alternativ können Sie die geplante Aufgabe auch manuell ausführen, indem Sie **Taskplaner** (taskschd. msc) öffnen, zu **Taskplaner Bibliothek > Microsoft > Windows > hgsserver** navigieren und die Aufgabe mit dem Namen **attestationsignercertrenewaltask** ausführen.

Wechseln der Nachweis Modi

Wenn Sie HGS vom TPM-Modus in den Active Directory Modus wechseln oder umgekehrt mithilfe des Cmdlets [Set-hgsserver](#), kann es bis zu 10 Minuten dauern, bis jeder Knoten in Ihrem HGS-Cluster mit der Erzwingung des neuen Nachweis Modus beginnt. Dies ist das normale Verhalten. Es wird empfohlen, dass Sie keine Richtlinien entfernen, die Hosts aus dem vorherigen Nachweis Modus zulassen, bis Sie überprüft haben, ob alle Hosts erfolgreich mit dem neuen Nachweis Modus getestet wurden.

Bekanntes Problem beim Wechsel von TPM in den AD-Modus

Wenn Sie Ihren HGS-Cluster im TPM-Modus initialisiert und später in den Active Directory-Modus gewechselt haben, liegt ein bekanntes Problem vor, das verhindert, dass andere Knoten in Ihrem HGS-Cluster in den neuen Nachweis Modus wechseln. Um sicherzustellen, dass alle HGS-Server den richtigen Nachweis Modus erzwingen, führen Sie `Set-HgsServer -TrustActiveDirectory` **auf jedem Knoten** des HGS-Clusters aus. Dieses Problem tritt nicht auf, wenn Sie vom TPM-Modus in den AD - Modus wechseln und der Cluster ursprünglich im AD-Modus eingerichtet wurde.

Sie können den Nachweis Modus Ihres HGS-Servers durch Ausführen von [Get-hgsserver](#) überprüfen.

Verschlüsselungsrichtlinien für den Speicher Abbild

Wenn Sie versuchen, Speicher Abbild-Verschlüsselungsrichtlinien zu konfigurieren und die standardmäßigen HGS-dump Richtlinien (HGS_nodumps, HGS_dumpencryption und HGS_dumpverschlüsselungkey) oder das dump Richtlinien cmdlet (Add-hgsattestationdumpolicy) nicht zu sehen, ist es wahrscheinlich, dass das neueste kumulative Update nicht installiert ist [Aktualisieren Sie den HGS-Server](#) auf das neueste kumulative Windows

Update, und [Aktivieren Sie die neuen Nachweis Richtlinien](#), um dies zu beheben. Stellen Sie sicher, dass Sie Ihre Hyper-V-Hosts auf das gleiche kumulative Update aktualisieren, bevor Sie die neuen Nachweis Richtlinien aktivieren, da Hosts, auf denen die neuen dumpverschlüsselungs Funktionen nicht installiert sind, möglicherweise nach dem Aktivieren der HGS-Richtlinie fehlschlagen.

Fehlermeldungen für den Endorsement Key-Zertifikat

Beim Registrieren eines Hosts mithilfe des Cmdlets [Add-hgsattestationtpmhost](#) werden zwei TPM-IDs aus der bereitgestellten Plattform-bezeichnerdatei extrahiert: das Endorsement Key-Zertifikat (ekcert) und der Public Endorsement Key (ekpub). Das ekcert identifiziert den Hersteller des TPM und stellt sicher, dass das TPM authentisch ist und über die normale Lieferkette gefertigt wird. Das ekpub identifiziert dieses bestimmte TPM eindeutig und ist eines der Measures, die HGS verwendet, um einem Host Zugriff zum Ausführen von abgeschirmten VMS zu gewähren.

Beim Registrieren eines TPM-Hosts wird eine Fehlermeldung angezeigt, wenn eine der beiden Bedingungen erfüllt ist:

1. Die Plattform-bezeichnerdatei enthält **kein** Endorsement Key-Zertifikat.
2. Die Plattform-bezeichnerdatei enthält ein Endorsement Key-Zertifikat, aber dieses Zertifikat ist auf dem System **nicht vertrauenswürdig**.

Bestimmte TPM-Hersteller enthalten keine ekcerts in ihren TPMs. Wenn Sie vermuten, dass dies bei Ihrem TPM der Fall ist, vergewissern Sie sich bei Ihrem OEM, dass die TPMs kein ekcert aufweisen sollten, und verwenden Sie das `-Force`-Flag, um den Host manuell bei HGS zu registrieren. Wenn Ihr TPM über ein ekcert verfügen soll, aber in der Datei mit der Plattform Kennung nicht gefunden wurde, stellen Sie sicher, dass Sie beim Ausführen von "[Get-plattformidentifizier](#)" auf dem Host eine Administrator-PowerShell-Konsole (erweitert) verwenden.

Wenn Sie die Fehlermeldung erhalten, dass Ihr ekcert nicht vertrauenswürdig ist, stellen Sie sicher, dass Sie [das vertrauenswürdige TPM](#) -Stamm Zertifikat Paket auf jedem HGS-Server installiert haben und dass das Stamm Zertifikat für den TPM-Hersteller im Trust `dtpm-_rootca` -Speicher des lokalen Computers vorhanden ist. Alle anwendbaren zwischen Zertifikate müssen auch im Trust `dtpm-_intermediateca` -Speicher auf dem lokalen Computer installiert werden. Nachdem Sie die Stamm-und zwischen Zertifikate installiert haben, sollten Sie `Add-HgsAttestationTpmHost` erfolgreich ausführen können.

Problembehandlung für geschützte Hosts

09.04.2020 • 11 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

In diesem Thema werden Lösungen für häufige Probleme beschrieben, die beim Bereitstellen oder betreiben eines geschützten Hyper-V-Hosts in Ihrem geschützten Fabric auftreten. Wenn Sie sich nicht sicher sind, welche Art von Problem Sie haben, versuchen Sie zunächst, die [geschützte Fabric-Diagnose](#) auf Ihren Hyper-V-Hosts auszuführen, um die möglichen Gründe einzugrenzen.

Überwachte Host Funktion

Wenn Probleme mit dem Hyper-v-Host auftreten, stellen Sie zunächst sicher, dass die **Hyper-v-Unterstützung des Host** -Überwachungs Diensts installiert ist. Ohne dieses Feature fehlen dem Hyper-V-Host einige wichtige Konfigurationseinstellungen und Software, mit denen er den Nachweis durchlaufen und abgeschirmte VMS bereitstellen kann.

Verwenden Sie Server-Manager, oder führen Sie den folgenden Befehl in einem PowerShell-Fenster mit erhöhten Rechten aus:

```
Get-WindowsFeature HostGuardian
```

Wenn das Feature nicht installiert ist, installieren Sie es mit dem folgenden PowerShell-Befehl:

```
Install-WindowsFeature HostGuardian -Restart
```

Nachweis Fehler

Wenn ein Host den Nachweis nicht mit dem Host-Überwachungsdienst übergibt, ist es nicht möglich, abgeschirmte VMS auszuführen. Die Ausgabe von [Get-hgsclientconfiguration](#) auf diesem Host zeigt Informationen darüber an, warum bei diesem Host ein Fehler aufgetreten ist.

In der folgenden Tabelle werden die Werte erläutert, die ggf. im Feld **attestationstatus** und mögliche nächste Schritte angezeigt werden können.

| ATTESTATIONSTATUS | ERKLÄRUNG |
|---------------------------|---|
| Abgelaufen | Der Host hat den Nachweis zuvor übermittelt, das ausgegebene Integritäts Zertifikat ist jedoch abgelaufen. Stellen Sie sicher, dass die Host-und HGS-Zeit synchronisiert sind. |
| Insecurehostconfiguration | Der Host hat den Nachweis nicht bestanden, weil er nicht den Nachweis Richtlinien entsprach, die auf HGS konfiguriert sind. Weitere Informationen finden Sie in der Tabelle attestationsubstatus. |

| ATTESTATIONSTATUS | ERKLÄRUNG |
|-------------------|---|
| NotConfigured | Der Host ist nicht für die Verwendung eines HGS für den Nachweis und den Schlüsselschutz konfiguriert. Stattdessen ist Sie für den lokalen Modus konfiguriert. Wenn sich dieser Host in einem geschützten Fabric befindet, verwenden Sie Set-hgsclientconfiguration , um die URLs für Ihren HGS-Server bereitzustellen. |
| Bestanden | Der Host hat den Nachweis übermittelt. |
| Transiendterror | Der letzte Nachweis Versuch ist aufgrund eines Netzwerk-, Dienst-oder anderen temporären Fehlers fehlgeschlagen. Wiederholen Sie den letzten Vorgang. |
| Tpmerror | Der Host konnte den letzten Nachweis Versuch aufgrund eines Fehlers mit dem TPM nicht durchführen. Weitere Informationen finden Sie in den TPM-Protokollen. |
| Unauthorizedhost | Der Host hat den Nachweis nicht bestanden, weil er nicht zum Ausführen von abgeschirmten VMS autorisiert ist. Stellen Sie sicher, dass der Host zu einer Sicherheitsgruppe gehört, die von HGS als vertrauenswürdig eingestuft wird |
| Unbekannt | Der Host hat noch nicht versucht, HGS zu bestätigen. |

Wenn **attestationstatus** als **insecurehostconfiguration** gemeldet wird, werden im Feld **attestationsubstatus** ein oder mehrere Gründe aufgefüllt. In der folgenden Tabelle werden die möglichen Werte für attestationsubstatus und Tipps zum Beheben des Problems erläutert.

| ATTESTATIONSUBSTATUS | BEDEUTUNG UND VORGEHENSWEISE |
|----------------------|---|
| BitLocker | Das Betriebssystem Volume des Hosts wird nicht von BitLocker verschlüsselt. Um dieses Problem zu beheben, Aktivieren Sie BitLocker auf dem Betriebssystem Volume, oder Deaktivieren Sie die BitLocker-Richtlinie auf HGS . |
| Codeintegritypolicy | Der Host ist nicht für die Verwendung einer Code Integritätsrichtlinie konfiguriert oder verwendet keine Richtlinie, die vom HGS-Server als vertrauenswürdig eingestuft wird. Stellen Sie sicher, dass eine Code Integritätsrichtlinie konfiguriert wurde, dass der Host neu gestartet wurde und die Richtlinie beim HGS-Server registriert ist. Weitere Informationen finden Sie unter Erstellen und Anwenden einer Code Integritätsrichtlinie . |
| Dumpsenabled | Der Host ist so konfiguriert, dass Absturz Abbilder oder Live-Speicher Abbilder zugelassen werden, was von ihren HGS-Richtlinien nicht zulässig ist. Um dieses Problem zu beheben, deaktivieren Sie Abbilder auf dem Host. |
| Dumpencryption | Der Host ist so konfiguriert, dass Absturz Abbilder oder Live-Speicher Abbilder zugelassen werden, aber diese Abbilder nicht verschlüsselt werden. Deaktivieren Sie entweder Abbilder auf dem Host, oder konfigurieren Sie die dumpverschlüsselung . |

| ATTESTATIONSUBSTATUS | BEDEUTUNG UND VORGEHENSWEISE |
|---------------------------------------|--|
| Dumpverschlüsselungskey | Der Host ist so konfiguriert, dass er Dumps zulässt und verschlüsselt, verwendet aber kein Zertifikat, das HGS bekannt ist, um Sie zu verschlüsseln. Um dieses Problem zu beheben, Aktualisieren Sie den Verschlüsselungsschlüssel für die Sicherung auf dem Host, oder registrieren Sie den Schlüssel bei HGS . |
| Voll Start | Der Host wurde aus dem Ruhezustand oder dem Ruhezustand fortgesetzt. Starten Sie den Host neu, damit ein sauberer, vollständiger Start ermöglicht wird. |
| Ruhe Zustands fähig | Der Host ist so konfiguriert, dass er den Ruhezustand zulässt, ohne die Ruhe Zustands Datei zu verschlüsseln, was von ihren HGS-Richtlinien nicht zulässig ist. Deaktivieren Sie den Ruhezustand, starten Sie den Host neu, oder konfigurieren Sie die dumpverschlüsselung . |
| Hypervisorenforcedcodeintegritypolicy | Der Host ist nicht für die Verwendung einer durch Hypervisor erzwungenen Code Integritätsrichtlinie konfiguriert. Überprüfen Sie, ob die Code Integrität vom Hypervisor aktiviert, konfiguriert und erzwungen wird. Weitere Informationen finden Sie im Device Guard-Bereitstellungs Handbuch . |
| IOMMU | Die virtualisierungsbasierten Sicherheitsfeatures des Hosts sind nicht so konfiguriert, dass ein IOMMU-Gerät zum Schutz vor Angriffen für den direkten Speicherzugriff erforderlich ist, wie dies für Ihre HGS-Richtlinien erforderlich ist. Vergewissern Sie sich, dass der Host über ein IOMMU verfügt, dass er aktiviert ist und dass Device Guard so konfiguriert ist, dass beim Starten von VSB der DMA-Schutz erforderlich ist. |
| Pagefileencryption | Die Verschlüsselung der Auslagerungs Datei ist auf dem Host nicht aktiviert. Um dieses Problem zu beheben, führen Sie <code>fsutil behavior set encryptpagingfile 1</code> aus, um die Verschlüsselung der Datei zu aktivieren. Weitere Informationen finden Sie unter "f"- Verhalten . |
| SecureBoot | Der sichere Start ist auf diesem Host nicht aktiviert oder verwendet nicht die Microsoft-Vorlage für den sicheren Start. Aktivieren Sie den sicheren Start mit der Microsoft Secure Boot-Vorlage, um dieses Problem zu beheben. |
| Securebootsettings | Die TPM-Baseline auf diesem Host entspricht keiner der von HGS als vertrauenswürdig eingestuft. Dies kann vorkommen, wenn Ihre UEFI-Start-, dbx-, Debug-oder benutzerdefinierten Richtlinien für den sicheren Start durch die Installation neuer Hardware oder Software geändert werden. Wenn Sie die aktuelle Hardware, Firmware und Softwarekonfiguration dieses Computers als vertrauenswürdig einstufen, können Sie eine neue TPM-Baseline erfassen und bei HGS registrieren . |

| ATTESTATIONSUBSTATUS | BEDEUTUNG UND VORGEHENSWEISE |
|----------------------|---|
| Tcglogverifizierung | Das TCG-Protokoll (TPM-Baseline) kann nicht abgerufen oder überprüft werden. Dies kann auf ein Problem mit der Firmware des Hosts, dem TPM oder anderen Hardwarekomponenten hinweisen. Wenn der Host für den PXE-Start konfiguriert ist, bevor Windows gestartet wird, kann auch ein veraltetes net Start Programm (NBP) diesen Fehler verursachen. Stellen Sie sicher, dass alle NBPs auf dem neuesten Stand sind, wenn PXE-Start aktiviert ist. |
| Virtualsecuremode | Auf dem Host werden keine virtualisierungsbasierten Sicherheitsfunktionen ausgeführt. Stellen Sie sicher, dass VSB aktiviert ist und dass Ihr System den konfigurierten Sicherheitsfeatures der Plattform entspricht. Weitere Informationen zu den VSB-Anforderungen finden Sie in der Device Guard-Dokumentation . |

Modernes TLS

Wenn Sie eine Gruppenrichtlinie bereitgestellt oder den Hyper-V-Host anderweitig konfiguriert haben, um die Verwendung von TLS 1,0 zu verhindern, kann der Fehler "der Host-Überwachungsdienst Client konnte eine Schlüssel Schutzvorrichtung im Auftrag eines aufrufenden Prozesses nicht entpacken" beim Versuch, eine abgeschirmte VM zu starten, angezeigt werden. Dies ist auf ein Standardverhalten in .NET 4,6 zurückzuführen, bei dem die standardmäßige TLS-Version des Systems beim Aushandeln unterstützter TLS-Versionen mit dem HGS-Server nicht berücksichtigt wird.

Um dieses Verhalten zu umgehen, führen Sie die folgenden beiden Befehle aus, um .net so zu konfigurieren, dass die standardmäßigen TLS-Versionen für alle .net-apps verwendet werden.

```
reg add HKLM\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 /v SystemDefaultTlsVersions /t REG_DWORD /d 1 /f
/reg:64
reg add HKLM\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 /v SystemDefaultTlsVersions /t REG_DWORD /d 1 /f
/reg:32
```

WARNING

Die Standardeinstellung für die TLS-Version des Systems wirkt sich auf alle .net-apps auf Ihrem Computer aus. Stellen Sie sicher, dass Sie die Registrierungsschlüssel in einer isolierten Umgebung testen, bevor Sie Sie auf den Produktions Computern bereitstellen.

Weitere Informationen zu .NET 4,6 und TLS 1,0 finden Sie unter [Lösen des TLS 1,0-Problems, 2. Edition](#).

Problembehandlung bei abgeschirmten VMS

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Ab Windows Server Version 1803 werden der erweiterte Sitzungs Modus (Virtual Machine Connection, VMConnect) und PS Direct für vollständig abgeschirmte VMS erneut aktiviert. Der Virtualisierungsadministrator benötigt trotzdem VM-Gast Anmelde Informationen, um Zugriff auf den virtuellen Computer zu erhalten. Dadurch wird es für einen Host jedoch einfacher, Probleme mit einer abgeschirmten VM zu beheben, wenn die Netzwerkkonfiguration beschädigt ist.

Um VMConnect und PS Direct für Ihre abgeschirmten VMS zu aktivieren, verschieben Sie Sie einfach auf einen Hyper-V-Host, auf dem Windows Server, Version 1803 oder höher, ausgeführt wird. Die virtuellen Geräte, die diese Features zulassen, werden automatisch erneut aktiviert. Wenn eine abgeschirmte VM auf einen Host verschoben wird, auf dem eine frühere Version von Windows Server ausgeführt wird, werden VMConnect und PS Direct erneut deaktiviert.

Für sicherheitsrelevante Kunden, die sich Gedanken darüber machen, ob Hoster Zugriff auf die VM haben und zum ursprünglichen Verhalten zurückkehren möchten, sollten die folgenden Funktionen im Gast Betriebssystem deaktiviert werden:

- Deaktivieren Sie den PowerShell Direct-Dienst auf dem virtuellen Computer:

```
Stop-Service vmicvmsession  
Set-Service vmicvmsession -StartupType Disabled
```

- Der erweiterte VMConnect-Sitzungs Modus kann nur deaktiviert werden, wenn Ihr Gast Betriebssystem mindestens Windows Server 2019 oder Windows 10, Version 1809, entspricht. Fügen Sie den folgenden Registrierungsschlüssel in Ihrem virtuellen Computer hinzu, um VMConnect-Verbindungen mit erweiterten Sitzungs Konsolen zu deaktivieren:

```
reg add "HKLM\Software\Microsoft\Virtual Machine\Guest" /v DisableEnhancedSessionConsoleConnection /t  
REG_DWORD /d 1
```


Integritätsnachweis für Geräte

09.04.2020 • 17 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

Der mit Windows 10, Version 1507, eingeführte Integritätsnachweis für Geräte (Device Health Attestation, DHA) weist folgende Merkmale auf:

- Integration in Windows 10 Mobile Device Management-Framework (MDM, Mobile Geräteverwaltung) in Ausrichtung mit [Open Mobile Alliance Standards \(OMA\)](#).
- Unterstützung von Geräten, die über eine in einer Firmware oder einem diskreten Format bereitgestellte Trusted Module Platform (TPM) verfügen.
- Ermöglicht Unternehmen, mit minimalem oder keinem Einfluss auf die Betriebskosten das Sicherheitsniveau ihrer Organisation auf hardwareüberwachte und -bescheinigte Sicherheit anzuheben.

Ab Windows Server 2016 können Sie den DHA-Dienst als Serverrolle in Ihrer Organisation ausführen. Nutzen Sie dieses Thema, um das Installieren und Konfigurieren der DHA-Serverrolle zu lernen.

Übersicht

Mit DHA können Sie den Integritätsnachweis für Geräte führen für:

- Windows 10 und mobile Geräte unter Windows 10, die TPM 1.2 oder 2.0 unterstützen.
- Lokale Geräte, die von Active Directory mit Internetzugriff verwaltet werden, Geräte, die von Active Directory ohne Internetzugriff verwaltet werden, Geräte, die von Azure Active Directory oder einer Hybridbereitstellung sowohl mit Active Directory als auch Azure Active Directory verwaltet werden.

DHA-Dienst

Der DHA-Dienst überprüft die TPM- und PCR-Protokolle für ein Gerät und generiert dann einen DHA-Bericht. Microsoft bietet den DHA-Dienst auf drei Arten an:

- **DHA-Clouddienst:** Ein von Microsoft verwalteter DHA-Dienst, der frei, einem geografischen Lastenausgleich unterzogen und für den Zugriff aus verschiedenen Weltregionen optimiert ist.
- **Lokaler DHA-Dienst:** Eine neue, mit Windows Server 2016 eingeführte Serverrolle. Er ist kostenlos für Kunden, die über eine Windows Server 2016-Lizenz verfügen.
- **DHA-Azure-Clouddienst:** Ein virtueller Host in Microsoft Azure. Zu diesem Zweck benötigen Sie einen virtuellen Host und Lizenzen für den lokalen DHA-Dienst.

Der DHA-Dienst ist in MDM-Lösungen integriert und bietet Folgendes:

- Kombinieren der Informationen, die sie von Geräten (über vorhandene Geräteverwaltungs-Kommunikationskanäle) mit dem DHA-Bericht erhalten
- Treffen einer sichereren und vertrauenswürdigeren Sicherheitsentscheidung auf Basis der hardwarebescheinigten und -geschützten Daten

Hier ist ein Beispiel, das zeigt, wie Sie DHA nutzen können, um das Sicherheitsniveau für die Ressourcen Ihrer Organisation anzuheben.

1. Sie erstellen eine Richtlinie, die die folgende(n) Startkonfiguration/-attribute überprüft:

- Sicherer Start
 - BitLocker
 - ELAM
2. Die MDM-Lösung erzwingt diese Richtlinie und löst eine auf den DHA-Berichtsdaten basierende Korrekturmaßnahme aus. Beispielsweise könnte sie Folgendes überprüfen:
- Der sichere Start wurde aktiviert, das Gerät lud vertrauenswürdigen, authentischen Code, und das Windows-Startladeprogramm wurde nicht manipuliert.
 - Vertrauenswürdiger Start überprüfte erfolgreich die digitale Signatur des Windows-Kernels und die Komponenten, die geladen wurden, während das Gerät startete.
 - Kontrollierter Start erstellte einen TPM-geschützten Audit-Trail, der remote überprüft werden konnte.
 - BitLocker wurde aktiviert und schützte die Daten, als das Gerät ausgeschaltet wurde.
 - ELAM wurde in frühen Startphasen aktiviert und überwacht die Laufzeit.

DHA-Clouddienst

Der DHA-Clouddienst bietet folgende Vorteile:

- Überprüfung der TCG- und PCR-Gerätestartprotokolle, die er von einem Gerät empfängt, das mit einer MDM-Lösung registriert ist.
- Erstellen eines manipulationssicheren Berichts (DHA-Bericht), der beschreibt, wie das Gerät auf der Basis von Daten startete, die von einem TPM-Chip des Geräts gesammelt und geschützt wurden.
- Übermitteln des DHA-Berichts an den MDM-Server, der den Bericht in einem geschützten Kommunikationskanal angefordert hat.

Lokaler DHA-Dienst

Der lokale DHA-Dienst bietet alle Funktionen, die auch der DHA-Clouddienst bietet. Außerdem ermöglicht er Kunden Folgendes:

- Optimieren der Leistung durch Ausführung des DHA-Diensts in Ihrem eigenen Rechenzentrum
- Sicherstellen, dass der DHA-Bericht nicht Ihr Netzwerk verlässt

DHA-Azure-Clouddienst

Dieser Dienst bietet die gleiche Funktionalität wie der lokale DHA-Dienst, mit der Ausnahme, dass der DHA-Azure-Clouddienst als virtueller Host in Microsoft Azure ausgeführt wird.

DHA-Validierungsmodi

Sie können den lokalen DHA-Dienst entweder zur Ausführung im EKCert- oder AIKCert-Validierungsmodus einrichten. Wenn der DHA-Dienst einen Bericht ausgibt, wird angezeigt, ob er im AIKCert- oder EKCert-Validierungsmodus ausgegeben wurde. AIKCert- und EKCert-Validierungsmodus bieten die gleiche Sicherheitsgarantie, solange die EKCert-Zertifikatkette auf dem neuesten Stand gehalten wird.

EKCert-Validierungsmodus

Der EKCert-Validierungsmodus ist optimiert für Geräte in Unternehmen, die nicht mit dem Internet verbunden sind. Geräte, die eine Verbindung mit einem DHA-Dienst herstellen, der im EKCert-Validierungsmodus ausgeführt wird, haben **keinen** direkten Zugriff auf das Internet.

Wenn DHA im EKCert-Validierungsmodus ausgeführt wird, hängt DHA von einer unternehmensverwalteten Zertifikatkette ab, die gelegentlich (ca. 5 - 10 Mal pro Jahr) aktualisiert werden muss.

Microsoft veröffentlicht aggregierte Pakete von vertrauenswürdigen Stammzertifizierungsstellen und Zwischenzertifizierungsstellen für genehmigte TPM-Hersteller (sobald sie verfügbar sind) in einem öffentlich zugänglichen Archiv im CAB-Archiv. Sie müssen den Feed herunterladen, die Integrität überprüfen und das Zertifikat auf dem Server installieren, der den Integritätsnachweis für Geräte ausführt.

Ein Beispiel Archiv ist <https://go.microsoft.com/fwlink/?linkid=2097925>.

AIKCert-Validierungsmodus

Der AIKCert-Validierungsmodus ist optimiert für Betriebsumgebungen, die über Zugriff auf das Internet verfügen. Geräte, die eine Verbindung mit einem DHA-Dienst herstellen, der im AIKCert-Validierungsmodus ausgeführt wird, müssen direkten Zugriff auf das Internet haben und können ein AIK-Zertifikat von Microsoft bekommen.

Installieren und Konfigurieren des DHA-Diensts unter Windows Server 2016

Verwenden Sie die folgenden Abschnitte, um DHA unter Windows Server 2016 zu installieren und konfigurieren.

Erforderliche Komponenten

Um einen lokalen DHA-Dienst einzurichten und zu überprüfen, benötigen Sie Folgendes:

- Einen Server, auf dem Windows Server 2016 ausgeführt wird.
- (Mindestens) ein Windows 10-Clientgerät mit einer TPM (Version 1.2 oder 2.0), das sich im Zustand „klar/bereit“ befindet und den aktuellen Windows Insider-Build ausführt.
- Entscheiden Sie sich zwischen einer Ausführung im EKCert- oder AIKCert-Validierungsmodus.
- Die folgenden Zertifikate stehen zur Verfügung:
 - **DHA-SSL-Zertifikat:** Ein x.509-SSL-Zertifikat, das über eine Enterprise Trusted Root mit einem exportierbaren privaten Schlüssel verkettet ist. Dieses Zertifikat schützt DHA-Datenkommunikation im Transit einschließlich Server-zu-Server-Kommunikation (DHA-Dienst und MDM-Server) und Server-zu-Client-Kommunikation (DHA-Dienst und ein Windows 10-Gerät).
 - **DHA-Signaturzertifikat:** Ein x.509-Zertifikat, das über eine Enterprise Trusted Root mit einem exportierbaren privaten Schlüssel verkettet ist. Der DHA-Dienst verwendet dieses Zertifikat zum digitalen Signieren.
 - **DHA-Verschlüsselungszertifikat:** Ein x.509-Zertifikat, das über eine Enterprise Trusted Root mit einem exportierbaren privaten Schlüssel verkettet ist. Der DHA-Dienst verwendet dieses Zertifikat auch zur Verschlüsselung.

Installieren von Windows Server 2016

Installieren Sie Windows Server 2016 mithilfe Ihrer bevorzugten Installationsmethode, wie z.B. Windows-Bereitstellungsdienste, oder Ausführen des Installationsprogramms von startbaren Medien, einem USB-Laufwerk oder dem lokalen Dateisystem. Wenn Sie jetzt zum ersten Mal den lokalen DHA-Dienst konfigurieren, sollten Sie Windows Server 2016 mit der Installationsoption **Desktopdarstellung** installieren.

Hinzufügen der Serverrolle „Integritätsnachweis für Geräte“

Sie können die Serverrolle „Integritätsnachweis für Geräte“ und ihre Abhängigkeiten mithilfe des Server-Managers installieren.

Nachdem Sie Windows Server 2016 installiert haben, wird das Gerät neu gestartet und der Server-Manager geöffnet. Wenn der Server-Manager nicht automatisch startet, klicken Sie auf **Start** und dann auf **Server-Manager**.

1. Klicken Sie auf **Rollen und Features** hinzufügen.
2. Klicken Sie auf der Seite **Bevor Sie beginnen** auf **Weiter**.
3. Klicken Sie auf der Seite **Installationstyp auswählen** auf **Rollenbasierte oder featurebasierte Installation**, und klicken Sie anschließend auf **Weiter**.
4. Klicken Sie auf der Seite **Zielserver auswählen** auf **Einen Server aus dem Serverpool auswählen**, treffen Sie Ihre Wahl, und klicken Sie dann auf **Weiter**.
5. Aktivieren Sie auf der Seite **Serverrollen auswählen** das Kontrollkästchen **Integritätsnachweis für Geräte**.
6. Klicken Sie auf **Features hinzufügen**, um andere erforderliche Rollendienste und Features zu installieren.
7. Klicken Sie auf **Weiter**.
8. Klicken Sie auf der Seite **Features auswählen** auf **Weiter**.

9. Klicken Sie auf der Seite Rolle "**Webserver (IIS)**" auf **Weiter**.
10. Klicken Sie auf der Seite **Rollendienste auswählen** auf **Weiter**.
11. Klicken Sie auf der Seite **Integritätsnachweis für Geräte** auf **Weiter**.
12. Klicken Sie auf der Seite **Installationsauswahl bestätigen** auf **Installieren**.
13. Klicken Sie nach dem Abschluss der Installation auf **Schließen**.

Installieren der Signatur- und Verschlüsselungszertifikate

Installieren Sie mit dem folgenden Windows PowerShell-Skript die Signatur- und Verschlüsselungszertifikate. Weitere Informationen zum Fingerabdruck finden Sie unter Gewusst [wie: Abrufen des Fingerabdrucks eines Zertifikats](#).

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {$_.Thumbprint -like "<thumbprint>"}
$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName
$keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys\" + $keyname
icacls $keypath /grant <username>:R

#<thumbprint>: Certificate thumbprint for encryption certificate or signing certificate
#<username>: Username for web service app pool, by default IIS_IUSRS
```

Installieren des vertrauenswürdigen TPM-Stammzertifikatpakets

Um das vertrauenswürdige TPM-Stammzertifikatpaket zu installieren, müssen Sie es extrahieren, ggf. Zertifikatketten entfernen, die von Ihrer Organisation nicht als vertrauenswürdige eingestuft werden, und „setup.cmd“ ausführen.

Herunterladen des vertrauenswürdigen TPM-Stammzertifikatpakets

Vor der Installation des Zertifikat Pakets können Sie die aktuelle Liste der vertrauenswürdigen TPM-Stämme von <https://go.microsoft.com/fwlink/?linkid=2097925> herunterladen.

Wichtig: Stellen Sie vor der Installation des Pakets sicher, dass es von Microsoft digital signiert ist.

Extrahieren des vertrauenswürdigen Zertifikatpakets

Extrahieren Sie das vertrauenswürdige Zertifikatpaket durch Ausführen der folgenden Befehle.

```
mkdir .\TrustedTpm
expand -F:* .\TrustedTpm.cab .\TrustedTpm
```

Entfernen der Zertifikatketten für TPM-Hersteller, die von Ihrer Organisation *nicht* als vertrauenswürdige eingestuft werden (optional)

Löschen Sie die Ordner für alle Zertifikatketten von TPM-Herstellern, die von Ihrer Organisation nicht als vertrauenswürdige eingestuft werden.

Hinweis: Im AIK-Zertifikatmodus ist der Microsoft-Ordner zum Überprüfen der von Microsoft ausgestellten AIK-Zertifikate erforderlich.

Installieren des vertrauenswürdigen Zertifikatpakets

Installieren Sie das vertrauenswürdige Zertifikatpaket durch Ausführen des Setupskripts aus der CAB-Datei.

```
.\setup.cmd
```

Konfigurieren des Integritätsnachweises für Geräte

Sie können Windows PowerShell verwenden, um den lokalen DHA-Dienst zu konfigurieren.

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint <encryption> -SigningCertificateThumbprint  
<signing> -SslCertificateStoreName My -SslCertificateThumbprint <ssl> -SupportedAuthenticationSchema "<schema>"
```

```
#<encryption>: Thumbprint of the encryption certificate  
#<signing>: Thumbprint of the signing certificate  
#<ssl>: Thumbprint of the SSL certificate  
#<schema>: Comma-delimited list of supported schemas including AikCertificate, EkCertificate, and AikPub
```

Konfigurieren der Zertifikatketten-Richtlinie

Konfigurieren Sie die Zertifikatketten-Richtlinie durch Ausführen des folgenden Windows PowerShell-Skripts.

```
$policy = Get-DHASCertificateChainPolicy  
$policy.RevocationMode = "NoCheck"  
Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
```

DHA-Verwaltungsbefehle

Hier finden Sie einige Windows PowerShell-Beispiele, die Ihnen helfen können, den DHA-Dienst zu verwalten.

Erstmaliges Konfigurieren des DHA-Diensts

```
Install-DeviceHealthAttestation -SigningCertificateThumbprint "<HEX>" -EncryptionCertificateThumbprint "<HEX>"  
-SslCertificateThumbprint "<HEX>" -Force
```

Entfernen der DHA-Dienstkonfiguration

```
Uninstall-DeviceHealthAttestation -RemoveSslBinding -Force
```

Abrufen des aktiven Signaturzertifikats

```
Get-DHASActiveSigningCertificate
```

Festlegen des aktiven Signaturzertifikats

```
Set-DHASActiveSigningCertificate -Thumbprint "<hex>" -Force
```

Hinweis: Dieses Zertifikat muss auf dem Server bereitgestellt werden, der den DHA-Dienst im Zertifikatspeicher **LocalMachine\My** ausführt. Wenn das aktive Signaturzertifikat festgelegt ist, wird das vorhandene aktive Signaturzertifikat in die Liste der inaktiven Signaturzertifikate verschoben.

Liste der inaktiven Signaturzertifikate

```
Get-DHASInactiveSigningCertificates
```

Entfernen beliebiger inaktiver Signaturzertifikate

```
Remove-DHASInactiveSigningCertificates -Force  
Remove-DHASInactiveSigningCertificates -Thumbprint "<hex>" -Force
```

Hinweis: Nur *ein* inaktives Zertifikat (beliebigen Typs) kann zu einem beliebigen Zeitpunkt im Dienst vorhanden sein. Zertifikate sollten aus der Liste der inaktiven Zertifikate entfernt werden, sobald sie nicht mehr

benötigt werden.

Abrufen des aktiven Verschlüsselungszertifikats

```
Get-DHASActiveEncryptionCertificate
```

Festlegen des aktiven Verschlüsselungszertifikats

```
Set-DHASActiveEncryptionCertificate -Thumbprint "<hex>" -Force
```

Das Zertifikat muss auf dem Gerät im Zertifikatspeicher **LocalMachine\My** bereitgestellt werden.

Wenn das aktive Verschlüsselungszertifikat festgelegt ist, wird das vorhandene aktive Verschlüsselungszertifikat in die Liste der inaktiven Verschlüsselungszertifikate verschoben.

Liste der inaktiven Verschlüsselungszertifikate

```
Get-DHASInactiveEncryptionCertificates
```

Entfernen beliebiger inaktiver Verschlüsselungszertifikate

```
Remove-DHASInactiveEncryptionCertificates -Force  
Remove-DHASInactiveEncryptionCertificates -Thumbprint "<hex>" -Force
```

Abrufen der X509ChainPolicy-Konfiguration

```
Get-DHASCertificateChainPolicy
```

Ändern der X509ChainPolicy-Konfiguration

```
$certificateChainPolicy = Get-DHASInactiveEncryptionCertificates  
$certificateChainPolicy.RevocationFlag = <X509RevocationFlag>  
$certificateChainPolicy.RevocationMode = <X509RevocationMode>  
$certificateChainPolicy.VerificationFlags = <X509VerificationFlags>  
$certificateChainPolicy.UrlRetrievalTimeout = <TimeSpan>  
Set-DHASCertificateChainPolicy = $certificateChainPolicy
```

DHA-Dienstberichterstellung

Im Folgenden finden Sie eine Liste der Meldungen des DHA-Diensts an die MDM-Lösung:

- **200** HTTP OK. Das Zertifikat wird zurückgegeben.
- **400** Ungültige Anforderung. Ungültiges Anforderungsformat, ungültiges Integritätszertifikat, keine Übereinstimmung bei Zertifikatsignatur, ungültiges Integritätsnachweisblob oder ungültiges Integritätsstatusblob. Die Antwort enthält auch, wie im Antwortschema beschrieben, eine Nachricht mit einem Fehlercode und eine Fehlermeldung, die für die Diagnose verwendet werden kann.
- **500** Interner Serverfehler. Dies kann geschehen, wenn Probleme auftreten, die verhindern, dass der Dienst Zertifikate ausstellt.
- **503** Einschränkung lehnt Anforderungen ab, um eine Überlastung des Servers zu verhindern.

Anleitungen zur Deaktivierung von Systemdiensten unter Windows Server 2016 mit Desktopdarstellung

26.05.2020 • 99 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

Das Windows-Betriebssystem enthält viele Systemdienste, mit denen wichtige Funktionen bereitgestellt werden. Die Dienste verfügen über unterschiedliche Standardrichtlinien für den Start: einige werden standardmäßig gestartet (automatisch), einige bei Bedarf (manuell) und einige sind standardmäßig deaktiviert und müssen explizit aktiviert werden, bevor sie ausgeführt werden können. Diese Standardeinstellungen wurden für jeden Dienst sorgfältig gewählt, um für typische Kunden eine gute Abstimmung in Bezug auf Leistung, Funktionalität und Sicherheit zu erzielen.

Einige Unternehmenskunden ziehen für ihre Windows-PCs und -Server aber ggf. einen stärker auf Sicherheit ausgerichteten Ansatz vor, bei dem die Angriffsfläche auf das absolute Minimum reduziert ist. Diese Kunden möchten daher alle Dienste vollständig deaktivieren, die in ihren jeweiligen Umgebungen nicht benötigt werden. Für diese Kunden stellt Microsoft® diese Anleitung bereit, die Hinweise dazu enthält, welche Dienste zu diesem Zweck deaktiviert werden können.

Die Anleitung gilt nur für Windows Server 2016 mit Desktopdarstellung (nicht bei Nutzung als Desktopersatz für Endbenutzer). Ab Windows Server 2019 sind diese Richtlinien standardmäßig konfiguriert. Die Dienste des Systems sind jeweils wie folgt kategorisiert:

- **Deaktivierung empfohlen:** Für sicherheitsorientierte Unternehmen wird die Deaktivierung dieses Diensts und der Verzicht auf die damit verbundenen Funktionen in den meisten Fällen empfohlen (siehe zusätzliche Details unten).
- **Deaktivierung OK:** Dieser Dienst verfügt über Funktionen, die für einige Unternehmen nützlich sind. Er kann von sicherheitsorientierten Unternehmen, die ihn nicht nutzen, problemlos deaktiviert werden.
- **Nicht deaktivieren:** Wenn Dienste dieser Art deaktiviert werden, wirkt sich dies auf grundlegende Funktionen aus, oder es wird verhindert, dass bestimmte Rollen oder Features richtig funktionieren. Daher sollten sie nicht deaktiviert werden.
- **Kein Hinweis:** Die Auswirkungen der Deaktivierung dieser Dienste wurden noch nicht vollständig evaluiert. Aus diesem Grund sollte die Standardkonfiguration dieser Dienste nicht geändert werden.

Kunden können ihre Windows-PCs und -Server konfigurieren, um ausgewählte Dienste zu deaktivieren, indem sie die Sicherheitsvorlagen in ihren Gruppenrichtlinien oder die PowerShell-Automatisierung verwenden. In einigen Fällen umfasst die Anleitung bestimmte Gruppenrichtlinieneinstellungen, mit denen die Funktionen des Diensts direkt deaktiviert werden. Dies ist eine Alternative zum Deaktivieren des gesamten Diensts.

Microsoft empfiehlt Kunden die Deaktivierung der folgenden Dienste und der jeweiligen geplanten Aufgaben unter Windows Server 2016 mit Desktopdarstellung:

Dienste:

1. Xbox Live Authentifizierungs-Manager
2. Xbox Live-Spiele speichern

Geplante Aufgaben:

1. \Microsoft\XblGameSave\XblGameSaveTask
2. \Microsoft\XblGameSave\XblGameSaveTaskLogon

(Du kannst auf die Informationen zu allen Diensten in diesem Artikel auch zugreifen, indem du die angefügte Microsoft Excel-Tabelle anzeigst: [Anleitungen zur Deaktivierung von Systemdiensten unter Windows Server 2016 mit Desktopdarstellung](#).)

Deaktivieren von nicht standardmäßig installierten Diensten

Microsoft rät von der Anwendung von Richtlinien zum Deaktivieren von Diensten ab, die nicht standardmäßig installiert werden.

- Der Dienst wird in der Regel benötigt, wenn das Feature installiert ist. Für das Installieren des Diensts bzw. des Features sind Administratorrechte erforderlich. Lege nicht das Starten des Diensts als unzulässig fest, sondern das Installieren des Features.
- Durch das Blockieren des Microsoft Windows-Diensts wird nicht verhindert, dass ein Administrator (oder in einigen Fällen auch andere Benutzer) einen ähnlichen Dienst eines Drittanbieters installiert, der unter Umständen mit einem höheren Sicherheitsrisiko verbunden ist.
- Wenn ein nicht zum Standard gehörender Windows-Dienst (z. B. W3SVC) per Baseline oder Benchmark deaktiviert wird, erweckt dies bei einigen Prüfern den Eindruck, als ob die Technologie (z. B. IIS) grundsätzlich unsicher ist und niemals verwendet werden sollte.
- Wenn das Feature (und der Dienst) niemals installiert wird, macht dies die Baseline und den Prüfaufwand nur unnötig komplizierter.

Die beiden folgenden Tabellen enthalten für alle in diesem Dokument aufgeführten Dienste eine Beschreibung der Spalten und Microsoft-Empfehlungen zum Aktivieren und Deaktivieren von Systemdiensten unter Windows Server 2016 mit Desktopdarstellung:

Beschreibung der Spalten

| Dienstname | Schlüsselname (interner Name) des Diensts |
|--------------|---|
| Beschreibung | Die Beschreibung des Diensts aus „sc.exe qdescription“. |
| Installation | <i>Immer installiert:</i> Dienst ist unter Windows Server 2016 Core und Windows Server 2016 mit Desktopdarstellung installiert.
<i>Nur mit Desktopdarstellung:</i> Dienst ist unter Windows Server 2016 mit Desktopdarstellung, aber nicht unter Server Core installiert. |
| Starttyp | Starttyp des Diensts unter Windows Server 2016 |
| Empfehlung | Empfehlung/Hinweis von Microsoft zur Deaktivierung dieses Diensts unter Windows Server 2016 bei einer typischen, gut verwalteten Unternehmensbereitstellung, bei der der Server nicht als Desktopersatz für den Endbenutzer verwendet wird. |
| Kommentare | Zusätzliche Beschreibung |

Beschreibung von Microsoft-Empfehlungen

| Nicht deaktivieren | Dieser Dienst sollte nicht deaktiviert werden. |
|--------------------|--|
| Deaktivierung OK | Dieser Dienst kann deaktiviert werden, wenn das von ihm unterstützte Feature nicht verwendet wird. |

| | |
|--------------------------------|---|
| Bereits deaktiviert | Dieser Dienst wird standardmäßig deaktiviert. Die Erzwingung per Richtlinie ist nicht erforderlich. |
| Deaktivierung empfohlen | Dieser Dienst sollte auf einem gut verwalteten Unternehmenssystem niemals aktiviert werden. |

Die folgenden Tabellen enthalten Microsoft-Anleitungen zum Deaktivieren von Systemdiensten unter Windows Server 2016 mit Desktopdarstellung:

ActiveX-Installationsprogramm (AxInstSV)

| | |
|---------------------|--|
| Dienstname | AxInstSV |
| Beschreibung | Ermöglicht die Überprüfung der Benutzerkontensteuerung für die Installation von ActiveX-Steuerelementen über das Internet und die Verwaltung der Installation von ActiveX-Steuerelementen basierend auf Gruppenrichtlinieneinstellungen. Dieser Dienst wird bedarfsgesteuert gestartet, und wenn er deaktiviert ist, verhält sich die Installation von ActiveX-Steuerelementen gemäß den Einstellungen des Standardbrowsers. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | Die Deaktivierung ist in Ordnung, wenn das Feature nicht benötigt wird. |

AllJoyn-Routerdienst

| | |
|---------------------|--|
| Dienstname | AJRouter |
| Beschreibung | Leitet AllJoyn-Mitteilungen für die lokalen AllJoyn-Clients um. Wenn dieser Dienst angehalten wird, können die AllJoyn-Clients, die nicht über eigene gebündelte Router verfügen, nicht ausgeführt werden. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

App-Bereitschaft

| | |
|--------------|---|
| | |
| Dienstname | AppReadiness |
| Beschreibung | Bereitet Apps für die Nutzung vor, wenn sich ein Benutzer zum ersten Mal am PC anmeldet und neue Apps hinzugefügt werden. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | |
| | |

Anwendungsidentität

| | |
|--------------|--|
| | |
| Dienstname | AppIDSvc |
| Beschreibung | Ermittelt und überprüft die Identität einer Anwendung. Wenn dieser Dienst deaktiviert wird, kann AppLocker nicht erzwungen werden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Anwendungsinformationen

| | |
|--------------|---|
| | |
| Dienstname | Appinfo |
| Beschreibung | Ermöglicht das Ausführen von interaktiven Anwendungen mit zusätzlichen Administratorrechten. Wenn dieser Dienst beendet wird, können Benutzer keine Anwendungen mit den zusätzlichen Administratorrechten mehr starten, die sie für bestimmte Benutzeraufgaben unter Umständen benötigen. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |

| | |
|-------------------|---|
| | |
| Empfehlung | Kein Hinweis |
| Kommentare | Unterstützt die Rechteerweiterung für die Benutzerkontensteuerung auf demselben Desktop |
| | |

Gatewaydienst auf Anwendungsebene

| | |
|---------------------|--|
| | |
| Dienstname | ALG |
| Beschreibung | Stellt Unterstützung für Drittanbieterprotokoll-Plug-Ins für die gemeinsame Nutzung der Internetverbindung bereit. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Anwendungsverwaltung

| | |
|---------------------|--|
| | |
| Dienstname | AppMgmt |
| Beschreibung | Verarbeitet Installations-, Entfernungs und Enumerationsanforderungen für Software, die über die Gruppenrichtlinie bereitgestellt wird. Wenn der Dienst deaktiviert wird, können Benutzer keine Software mehr installieren, entfernen oder enumerieren, die per Gruppenrichtlinie bereitgestellt wird. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

AppX-Bereitstellungsdienst (AppXSVC)

| | |
|--------------|--|
| | |
| Dienstname | AppXSvc |
| Beschreibung | Stellt Infrastrukturunterstützung für die Bereitstellung von Store-Anwendungen bereit. Dieser Dienst wird bedarfsgesteuert gestartet. Wenn er deaktiviert wird, werden Store-Anwendungen nicht für das System bereitgestellt und funktionieren ggf. nicht richtig. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Automatische Zeitzoneaktualisierung

| | |
|--------------|---|
| | |
| Dienstname | tzautoupdate |
| Beschreibung | Legt die Zeitzone des Systems automatisch fest. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Deaktiviert |
| Empfehlung | Bereits deaktiviert |
| Kommentare | |
| | |

Intelligenter Hintergrundübertragungsdienst (Background Intelligent Transfer Service, BITS)

| | |
|--------------|--|
| | |
| Dienstname | BITS |
| Beschreibung | Überträgt Dateien im Hintergrund, indem ungenutzte Netzwerkbandbreite verwendet wird. Wenn der Dienst deaktiviert wird, können alle Anwendungen, die von BITS abhängig sind, z. B. Windows Update oder MSN Explorer, Programme und andere Informationen nicht automatisch herunterladen. |
| Installation | Immer installiert |
| Starttyp | Manuell |

| | |
|------------|--------------|
| | |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Infrastrukturdienst für Hintergrundaufgaben

| | |
|--------------|--|
| | |
| Dienstname | BrokerInfrastructure |
| Beschreibung | Windows-Infrastrukturdienst, mit dem gesteuert wird, welche Hintergrundaufgaben auf dem System ausgeführt werden können. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Basisfiltermodul

| | |
|--------------|--|
| | |
| Dienstname | BFE |
| Beschreibung | Das Basisfiltermodul (Base Filtering Engine, BFE) ist ein Dienst, mit dem Firewall- und IPsec-Richtlinien (Internetprotokollsicherheit) verwaltet werden und die Benutzermodusfilterung implementiert wird. Wenn der BFE-Dienst beendet oder deaktiviert wird, bedeutet dies eine erhebliche Reduzierung der Systemsicherheit. Darüber hinaus führt dies zu unvorhersehbarem Verhalten von IPsec-Verwaltungs- und Firewallanwendungen. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Bluetooth-Unterstützungsdienst

| | |
|--------------|---|
| | |
| Dienstname | bthserv |
| Beschreibung | Der Bluetooth-Dienst unterstützt die Ermittlung und Zuordnung von externen Bluetooth-Geräten. Das Beenden oder Deaktivieren dieses Diensts kann dazu führen, dass bereits installierte Bluetooth-Geräte nicht mehr richtig funktionieren und verhindert wird, dass neue Geräte ermittelt oder zugeordnet werden können. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | Die Deaktivierung ist in Ordnung, wenn der Dienst nicht verwendet wird. Ein weiterer Mechanismus für die Deaktivierung:
https://technet.microsoft.com/library/dd252791.aspx |
| | |

CDPUserSvc

| | |
|--------------|---|
| | |
| Dienstname | CDPUserSvc |
| Beschreibung | Dieser Benutzerdienst wird für Szenarien mit der Plattform für verbundene Geräte verwendet. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Automatisch |
| Empfehlung | Deaktivierung OK |
| Kommentare | Benutzerdienstvorlage |
| | |

Zertifikatverteilung

| | |
|--------------|---|
| | |
| Dienstname | CertPropSvc |
| Beschreibung | Kopiert Benutzer- und Stammzertifikate von Smartcards in den Zertifikatspeicher des aktuellen Benutzers, erkennt das Einlegen einer Smartcard in einen Smartcardleser und installiert bei Bedarf den zugehörigen Plug & Play-Minitreiber. |
| Installation | Immer installiert |
| Starttyp | Manuell |

| | |
|-------------------|--------------|
| | |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Clientlizenzdienst (ClipSVC)

| | |
|---------------------|--|
| | |
| Dienstname | ClipSVC |
| Beschreibung | Stellt Infrastrukturunterstützung für den Microsoft Store bereit. Dieser Dienst wird bedarfsgesteuert gestartet, und wenn er deaktiviert wird, verhalten sich über den Microsoft Store gekaufte Anwendungen nicht korrekt. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

CNG-Schlüsselisolation

| | |
|---------------------|---|
| | |
| Dienstname | KeyIso |
| Beschreibung | Der CNG-Schlüsselisolationdienst wird im LSA-Prozess gehostet. Der Dienst stellt eine Schlüsselprozessisolation für private Schlüssel und zugehörige Kryptografievorgänge gemäß den Anforderungen der allgemeinen Kriterien bereit. Der Dienst speichert und verwendet langlebige Schlüssel in einem sicheren Prozess in Übereinstimmung mit den Anforderungen der allgemeinen Kriterien. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

COM+-Ereignissystem

| | |
|---------------------|--|
| | |
| Dienstname | EventSystem |
| Beschreibung | Unterstützt den Systemereignis-Benachrichtigungsdienst (SENS), mit dem Ereignisse automatisch an abonnierende COM-Komponenten verteilt werden. Nach dem Beenden des Diensts wird SENS geschlossen, so dass keine weiteren Anmelde- und Abmeldebenachrichtigungen bereitgestellt werden können. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

COM+-Systemanwendung

| | |
|---------------------|--|
| | |
| Dienstname | COMSysApp |
| Beschreibung | Verwaltet die Komponentenkonfiguration und -überwachung von COM+-basierten Komponenten. Nach dem Beenden des Diensts sind die meisten COM+-basierten Komponenten nicht ordnungsgemäß funktionsfähig. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Computerbrowser

| | |
|---------------------|---|
| | |
| Dienstname | Browser |
| Beschreibung | Führt eine aktuelle Liste der Computer im Netzwerk und gibt diese an als Browser fungierende Computer weiter. Diese Liste wird nicht aktualisiert oder gewartet, falls der Dienst beendet wird. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |

| | |
|--------------|---------------------|
| | |
| Installation | Immer installiert |
| Starttyp | Deaktiviert |
| Empfehlung | Bereits deaktiviert |
| Kommentare | |
| | |

Plattformdienst für verbundene Geräte

| | |
|--------------|---|
| | |
| Dienstname | CDPSvc |
| Beschreibung | Dieser Dienst wird für verbundene Geräte und Universal Glass-Szenarien verwendet. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Benutzererfahrung und Telemetrie im verbundenen Modus

| | |
|--------------|---|
| | |
| Dienstname | DiagTrack |
| Beschreibung | Durch den Dienst für Benutzererfahrung und Telemetrie im verbundenen Modus werden Features aktiviert, die Benutzerfreundlichkeit in Anwendungen und im verbundenen Modus unterstützen. Außerdem verwaltet dieser Dienst die ereignisgesteuerte Sammlung und Übertragung von Diagnose- und Nutzungsdaten (die zur Verbesserung der Benutzerfreundlichkeit und Qualität der Windows-Plattform eingesetzt werden). Dazu müssen die Diagnose- und Nutzungseinstellungen in der Datenschutzooption unter „Feedback und Diagnose“ aktiviert sein. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Kontaktdaten

| | |
|--------------|--|
| | |
| Dienstname | PimIndexMaintenanceSvc |
| Beschreibung | Indiziert Kontaktdaten für die schnelle Kontaktsuche. Wenn du diesen Dienst beendest oder deaktivierst, können Kontakte in den Suchergebnissen fehlen. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | Benutzerdienstvorlage |
| | |

CoreMessaging

| | |
|--------------|---|
| | |
| Dienstname | CoreMessagingRegistrar |
| Beschreibung | Verwaltet die Kommunikation zwischen Systemkomponenten. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Anmeldeinformationsverwaltung

| | |
|--------------|--|
| | |
| Dienstname | VaultSvc |
| Beschreibung | Ermöglicht die sichere Speicherung und den Abruf von Anmeldeinformationen für Benutzer, Anwendungen und Sicherheitspakete. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |

| | |
|--|--|
| | |
| | |

Kryptografiedienste

| | |
|--------------|---|
| | |
| Dienstname | CryptSvc |
| Beschreibung | Stellt drei Verwaltungsdienste bereit: den Katalogdatenbankendienst, der die Signaturen von Windows-Dateien bestätigt und die Installation neuer Programme ermöglicht, den geschützten Stammdienst, der diesem Computer vertrauenswürdige Zertifikate von Stammzertifizierungsstellen hinzufügt und diese vom Computer entfernt, und den automatischen Aktualisierungsdienst für die Stammzertifizierung, der Stammzertifikate vom Windows Update abrufen und Szenarien wie SSL aktivieren. Wird dieser Dienst beendet, funktionieren diese Verwaltungsdienste nicht ordnungsgemäß. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Datenfreigabedienst

| | |
|--------------|---|
| | |
| Dienstname | DsSvc |
| Beschreibung | Dient als Datenbroker zwischen Anwendungen. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

DataCollectionPublishingService

| | |
|------------|--------|
| | |
| Dienstname | DcpSvc |

| | |
|---------------------|---|
| | |
| Beschreibung | Der Dienst für die Erfassung und Veröffentlichung von Daten (Data Collection and Publishing, DCP) unterstützt Erstanbieter-Apps zum Hochladen von Daten in die Cloud. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

DCOM-Server-Prozessstart

| | |
|---------------------|---|
| | |
| Dienstname | DcomLaunch |
| Beschreibung | Der Dienst DCOMLAUNCH startet COM- und DCOM-Server als Reaktion auf Objektaktivierungsanforderungen. Wenn dieser Dienst beendet oder deaktiviert wird, funktionieren Programme, für die COM oder DCOM genutzt wird, nicht richtig. Wir empfehlen dir dringend, den Dienst DCOMLAUNCH auszuführen. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Gerätezuordnungsdienst

| | |
|---------------------|---|
| | |
| Dienstname | DeviceAssociationService |
| Beschreibung | Ermöglicht die Kopplung zwischen dem System und verkabelten Geräten oder Drahtlosgeräten. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Geräteinstallationsdienst

| | |
|--------------|--|
| | |
| Dienstname | DeviceInstall |
| Beschreibung | Ermöglicht einem Computer die Erkennung und Anpassung an Hardwareänderungen mit nur wenigen oder ganz ohne Benutzereingaben. Das Beenden oder Deaktivieren dieses Diensts führt zu Instabilität des Systems. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Registrierungsdienst für die Geräteverwaltung

| | |
|--------------|---|
| | |
| Dienstname | DmEnrollmentSvc |
| Beschreibung | Führt Aktivitäten der Geräteregistrierung für die Geräteverwaltung durch. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Geräteinstallations-Manager

| | |
|--------------|---|
| | |
| Dienstname | DsmSvc |
| Beschreibung | Ermöglicht die Erkennung, den Download und die Installation von gerätebezogener Software. Wenn dieser Dienst deaktiviert wird, werden die Geräte ggf. mit veralteter Software konfiguriert und funktionieren unter Umständen nicht richtig. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |

| | |
|------------|--|
| | |
| Kommentare | |
| | |

Broker für DevQuery-Hintergrundermittlung

| | |
|--------------|--|
| | |
| Dienstname | DevQueryBroker |
| Beschreibung | Ermöglicht Apps die Ermittlung von Geräten per Hintergrundaufgabe. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

DHCP-Client

| | |
|--------------|---|
| | |
| Dienstname | Dhcp |
| Beschreibung | Registriert und aktualisiert IP-Adressen und DNS-Einträge für diesen Computer. Wenn dieser Dienst beendet wird, empfängt der Computer keine dynamischen IP-Adressen und DNS-Updates mehr. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Diagnoserichtliniendienst

| | |
|--------------|---|
| | |
| Dienstname | DPS |
| Beschreibung | Der Diagnoserichtliniendienst ermöglicht die Problemerkennung, Problembehandlung und Lösung für Windows-Komponenten. Wenn dieser Dienst beendet wird, funktioniert die Diagnose nicht mehr. |

| | |
|--------------|-------------------|
| | |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Diagnosediensthost

| | |
|--------------|--|
| | |
| Dienstname | WdiServiceHost |
| Beschreibung | Der Diagnosediensthost wird vom Diagnoserichtliniendienst als Host für Diagnosen verwendet, die im Kontext eines lokalen Diensts ausgeführt werden müssen. Wird dieser Dienst beendet, funktionieren alle davon abhängigen Diagnosen nicht mehr ordnungsgemäß. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Diagnosesystemhost

| | |
|--------------|---|
| | |
| Dienstname | WdiSystemHost |
| Beschreibung | Der Diagnosesystemhost wird vom Diagnoserichtliniendienst verwendet, um Diagnosen zu hosten, die für einen lokalen Dienst durchgeführt werden müssen. Wird dieser Dienst beendet, funktionieren alle davon abhängigen Diagnosen nicht mehr ordnungsgemäß. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Überwachung verteilter Verknüpfungen (Client)

| | |
|--------------|---|
| | |
| Dienstname | TrkWks |
| Beschreibung | Verwaltet die Links zwischen NTFS-Dateien auf einem Computer oder für die Computer eines Netzwerks. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Distributed Transaction Coordinator

| | |
|--------------|---|
| | |
| Dienstname | MSDTC |
| Beschreibung | Koordiniert Transaktionen, die sich über mindestens zwei Ressourcenverwaltungen wie Datenbanken, Nachrichtenwarteschlangen oder Dateisysteme erstrecken. Wenn der Dienst beendet ist, treten bei diesen Transaktionen Fehler auf. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

dmwappushsvc

| | |
|--------------|-----------------------------------|
| | |
| Dienstname | dmwappushservice |
| Beschreibung | WAP Push-Nachrichtenroutingdienst |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |

| | |
|-------------------|---|
| | |
| Kommentare | Dieser Dienst wird auf Clientgeräten für Intune, MDM und ähnlichen Verwaltungstechnologien sowie für einheitliche Schreibfilter benötigt. Für Server ist der Dienst nicht erforderlich. |
| | |

DNS-Client

| | |
|---------------------|---|
| | |
| Dienstname | Dnscache |
| Beschreibung | Der DNS-Clientdienst (dnscache) wird zum Zwischenspeichern von DNS-Namen (Domain Name System) verwendet und registriert den vollständigen Computernamen für diesen Computer. Wenn der Dienst angehalten wird, werden DNS-Namen weiterhin aufgelöst. Die Ergebnisse von DNS-Namensabfragen werden jedoch nicht zwischengespeichert, und der Name des Computers wird nicht registriert. Wenn der Dienst deaktiviert wird, können Dienste, die explizit von diesem Dienst abhängig sind, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Manager für heruntergeladene Karten

| | |
|---------------------|--|
| | |
| Dienstname | MapsBroker |
| Beschreibung | Windows-Dienst für den Anwendungszugriff auf heruntergeladene Karten. Dieser Dienst wird bedarfsgesteuert je nach der Anwendung gestartet, die auf heruntergeladene Karten zugreift. Wenn der Dienst deaktiviert wird, können Apps nicht auf Karten zugreifen. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Automatisch |
| Empfehlung | Deaktivierung OK |
| Kommentare | Wenn der Dienst deaktiviert wird, funktionieren Apps nicht mehr, die den Dienst benötigen. Die Aktivierung ist kein Problem, wenn der Dienst von Apps nicht benötigt wird. |
| | |

Eingebetteter Modus

| | |
|--------------|---|
| | |
| Dienstname | embeddedmode |
| Beschreibung | Der Dienst „Eingebetteter Modus“ ermöglicht Szenarien, die sich auf Hintergrundanwendungen beziehen. Wenn dieser Dienst deaktiviert wird, wird die Aktivierung von Hintergrundanwendungen verhindert. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Verschlüsselndes Dateisystem (EFS)

| | |
|--------------|--|
| | |
| Dienstname | EFS |
| Beschreibung | Eine wichtige Dateiverschlüsselungstechnologie zum Speichern verschlüsselter Dateien auf Volumes mit dem Dateisystem NTFS. Wenn dieser Dienst beendet oder deaktiviert wird, können Anwendungen nicht mehr auf verschlüsselte Dateien zugreifen. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Verwaltungsdienst für Unternehmens-Apps

| | |
|--------------|--|
| | |
| Dienstname | EntAppSvc |
| Beschreibung | Ermöglicht die Verwaltung von Unternehmensanwendungen. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |

| | |
|------------|--|
| | |
| Kommentare | |
| | |

Extensible Authentication-Protokoll

| | |
|--------------|--|
| | |
| Dienstname | EapHost |
| Beschreibung | <p>Der EAP-Dienst (Extensible Authentication Protocol) stellt in folgenden Szenarios eine Netzwerkauthentifizierung bereit: 802.1X (verkabelt und drahtlos), VPN und NAP (Network Access Protection). EAP stellt darüber hinaus APIs (Application Programming Interface, Anwendungsprogrammierschnittstelle) bereit, die von Netzwerkzugriffclients, einschließlich Drahtlosclients und VPN-Clients, beim Authentifizierungsvorgang verwendet werden. Wenn du diesen Dienst deaktivierst, kann dieser Computer nicht mehr auf Netzwerke zugreifen, die eine EAP-Authentifizierung verwenden.</p> |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Funktionssuchanbieter-Host

| | |
|--------------|---|
| | |
| Dienstname | fdPHost |
| Beschreibung | <p>Der FDPHOST-Dienst dient zum Hosten der Netzwerkerkennungsanbieter für die Funktionssuche (Function Discovery, FD). Von diesen FD-Anbietern werden Netzwerkerkennungsdienste für das Simple Services Discovery-Protokoll (SSDP) und das Web Services – Discovery (WS-D)-Protokoll bereitgestellt. Durch das Beenden oder Deaktivieren des FDPHOST-Diensts wird bei Verwendung von FD die Netzwerkerkennung für diese Protokolle deaktiviert. Ist dieser Dienst nicht verfügbar, können mit Netzwerkdiensten, von denen FD und diese Erkennungsprotokolle verwendet werden, keine Netzwerkgeräte oder -ressourcen gesucht werden.</p> |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |

| | |
|------------|--|
| | |
| Kommentare | |
| | |

Funktionssuche-Ressourcenveröffentlichung

| | |
|--------------|--|
| | |
| Dienstname | FDResPub |
| Beschreibung | Veröffentlicht diesen Computer und die daran angeschlossenen Ressourcen, damit sie über das Netzwerk gesucht werden können. Wenn dieser Dienst beendet wird, werden die Netzwerkressourcen nicht mehr veröffentlicht, damit sie von anderen Computern im Netzwerk gesucht werden können. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Geolocation-Dienst

| | |
|--------------|--|
| | |
| Dienstname | lfsvc |
| Beschreibung | Dieser Dienst überwacht den aktuellen Standort des Systems und verwaltet Geofences (geografische Standorte mit zugeordneten Ereignissen). Wenn du diesen Dienst deaktivierst, sind Anwendungen nicht in der Lage, Benachrichtigungen zu Geolocations oder Geofences zu nutzen oder zu empfangen. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | Wenn der Dienst deaktiviert wird, funktionieren Apps nicht mehr, die den Dienst benötigen. Die Aktivierung ist kein Problem, wenn der Dienst von Apps nicht benötigt wird. |
| | |

Gruppenrichtlinienclient

| | |
|--------------|---|
| | |
| Dienstname | gpsvc |
| Beschreibung | Der Dienst ist für das Anwenden von Einstellungen verantwortlich, die über die Gruppenrichtlinienkomponente durch Administratoren für den Computer und die Benutzer konfiguriert wurden. Wenn der Dienst deaktiviert wird, werden die Einstellungen nicht angewendet. Somit können Anwendungen und Komponenten nicht über die Gruppenrichtlinie verwaltet werden. Von der Gruppenrichtlinienkomponente abhängige Komponenten oder Anwendungen funktionieren zudem ggf. nicht, wenn der Dienst deaktiviert wird. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Eingabegerätedienst

| | |
|--------------|--|
| | |
| Dienstname | hidserv |
| Beschreibung | Aktiviert und unterstützt die Verwendung von Abkürzungstasten auf Tastaturen, Fernbedienungen und anderen Multimediageräten. Wir empfehlen dir, diesen Dienst auszuführen. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

HV-Hostdienst

| | |
|--------------|--|
| | |
| Dienstname | HvHost |
| Beschreibung | Stellt eine Schnittstelle für den Hyper-V-Hypervisor bereit, um für das Hostbetriebssystem Leistungsindikatoren pro Partition verfügbar zu machen. |
| Installation | Immer installiert |

| | |
|------------|--|
| | |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Leistungsoptimierungen für Gast-VMs. Wird heutzutage meist nicht mehr verwendet (mit Ausnahme von explizit aufgefüllten VMs), aber der Dienst wird für Application Guard eingesetzt. |
| | |

Hyper-V-Datenaustauschdienst

| | |
|--------------|---|
| | |
| Dienstname | vmickvpexchange |
| Beschreibung | Stellt einen Mechanismus zum Austauschen von Daten zwischen dem virtuellen Computer und dem Betriebssystem bereit, das auf dem physischen Computer ausgeführt wird. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Siehe „HvHost“. |
| | |

Hyper-V-Gastdienstschnittstelle

| | |
|--------------|---|
| | |
| Dienstname | vmicguestinterface |
| Beschreibung | Stellt eine Schnittstelle für den Hyper-V-Host für die Interaktion mit bestimmten Diensten bereit, die auf dem virtuellen Computer ausgeführt werden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Siehe „HvHost“. |
| | |

Hyper-V-Dienst zum Herunterfahren des Gasts

| | |
|--------------|--|
| | |
| Dienstname | vmicshutdown |
| Beschreibung | Stellt einen Mechanismus zum Herunterfahren des Betriebssystems dieses virtuellen Computers über die Verwaltungsschnittstellen auf dem physischen Computer bereit. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Siehe „HvHost“. |
| | |

Hyper-V Taktdienst

| | |
|--------------|--|
| | |
| Dienstname | vmicheartbeat |
| Beschreibung | Überwacht den Zustand dieses virtuellen Computers, indem in regelmäßigen Abständen ein Heartbeat gemeldet wird. Mit diesem Dienst kannst du ausgeführte virtuelle Computer identifizieren, die nicht mehr reagieren. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Siehe „HvHost“. |
| | |

Hyper-V-Dienst PowerShell Direct

| | |
|--------------|--|
| | |
| Dienstname | vmicvmsession |
| Beschreibung | Stellt einen Mechanismus bereit, um einen virtuellen Computer mit PowerShell über eine VM-Sitzung ohne virtuelles Netzwerk zu verwalten. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |

| | |
|-------------------|-----------------|
| | |
| Kommentare | Siehe „HvHost“. |
| | |

Hyper-V-Remotedesktopvirtualisierungsdienst

| | |
|---------------------|--|
| | |
| Dienstname | vmicrdv |
| Beschreibung | Stellt eine Plattform für die Kommunikation zwischen dem virtuellen Computer und dem Betriebssystem bereit, das auf dem physischen Computer ausgeführt wird. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Siehe „HvHost“. |
| | |

Hyper-V-Zeitsynchronisierungsdienst

| | |
|---------------------|--|
| | |
| Dienstname | vmictimesync |
| Beschreibung | Synchronisiert die Systemzeit dieses virtuellen Computers mit der Systemzeit des physischen Computers. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Siehe „HvHost“. |
| | |

Hyper-V-Volumeschattenkopie-Anforderer

| | |
|---------------------|---|
| | |
| Dienstname | vmicvss |
| Beschreibung | Koordiniert die Kommunikation, die erforderlich ist, damit der Volumeschattenkopie-Dienst zum Sichern von Anwendungen und Daten auf diesem virtuellen Computer basierend auf dem Betriebssystem des physischen Computers verwendet werden kann. |

| | |
|--------------|--------------------|
| | |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Siehe „HvHost“. |
| | |

IKE- und AuthIP IPsec-Schlüsselerstellungsmodule

| | |
|--------------|---|
| | |
| Dienstname | IKEEXT |
| Beschreibung | Die IKEEXT-Diensthubs der Schlüsselerstellungsmodule für IKE (Internet Key Exchange) und Auth-IP (Authenticated Internet Protocol). Diese Schlüsselerstellungsmodule werden für die Authentifizierung und den Schlüsselaustausch in Internet Protocol Security (IPsec) verwendet. Wenn du den IKEEXT-Dienst anhältst oder deaktivierst, wird der IKE/AuthIP-Schlüsselaustausch mit Peercomputern deaktiviert. IPsec ist im Allgemeinen für die Verwendung von IKE/AuthIP konfiguriert, und das Anhalten oder Deaktivieren des IKEEXT-Diensts kann zu einem IPsec-Fehler führen und die Sicherheit des Systems gefährden. Wir empfehlen dir dringend, den Dienst IKEEXT auszuführen. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Erkennung interaktiver Dienste

| | |
|--------------|---|
| | |
| Dienstname | UI0Detect |
| Beschreibung | Aktiviert die Benutzerbenachrichtigung von Benutzereingaben für interaktive Dienste. Dies ermöglicht den Zugriff auf von interaktiven Diensten erstellte Dialogfelder, wenn diese angezeigt werden. Wenn dieser Dienst beendet wird, funktionieren Benachrichtigungen über neue interaktive Dienstdialogfelder nicht mehr, und der Zugriff auf Dialogfelder von interaktiven Diensten ist eventuell nicht möglich. Wenn dieser Dienst deaktiviert wird, funktionieren weder die Benachrichtigung über noch der Zugriff auf neue interaktive Dienstdialogfelder. |

| | |
|--------------|----------------------------|
| | |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Gemeinsame Nutzung der Internetverbindung

| | |
|--------------|--|
| | |
| Dienstname | SharedAccess |
| Beschreibung | Stellt die Dienste für die Netzwerkadressenübersetzung, Adressierung, Namensauflösung bzw. Verhinderung von Eindringversuchen für ein Heimnetzwerk oder ein Netzwerk eines kleinen Büros bereit. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | Ist für Clients erforderlich, die als WLAN-Hotspots genutzt werden, und außerdem an beiden Enden einer Miracast-Projektion. Die gemeinsame Nutzung der Internetverbindung kann mit der GPO-Einstellung „Verwendung der gemeinsam genutzten Internetverbindung im eigenen DNS-Domänennetzwerk nicht zulassen“ blockiert werden. |
| | |

IP-Hilfsprogramm

| | |
|--------------|--|
| | |
| Dienstname | iphlpvc |
| Beschreibung | Stellt Tunnelkonnektivität mithilfe von IPv6-Übergangstechnologien (IP6-zu-IP4, ISATAP, Portproxy und Teredo) und IP-HTTPS bereit. Wenn der Dienst beendet wird, verfügt der Computer nicht über die durch diese Technologien ermöglichten Konnektivitätsvorteile. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |

| | |
|--|--|
| | |
| | |

IPsec-Richtlinien-Agent

| | |
|--------------|--|
| | |
| Dienstname | PolicyAgent |
| Beschreibung | IPsec (Internetprotokollsicherheit) unterstützt die Peerauthentifizierung auf Netzwerkebene, die Datenursprungsauthentifizierung, die Datenintegrität, die Datenvertraulichkeit (Verschlüsselung) und den Replay-Schutz. Dieser Dienst erzwingt IPsec-Richtlinien, die mit dem Snap-In „IP-Sicherheitsrichtlinien“ oder dem Befehlszeilentool „netsh ipsec“ erstellt wurden. Wenn du diesen Dienst beendest, treten unter Umständen Probleme mit der Netzwerkkonnektivität auf, falls es für deine Richtlinie erforderlich ist, dass für Verbindungen IPsec genutzt wird. Darüber hinaus ist die Remoteverwaltung der Windows-Firewall nicht verfügbar, wenn dieser Dienst beendet wird. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

KDC-Proxyserverdienst (KPS)

| | |
|--------------|---|
| | |
| Dienstname | KPSSVC |
| Beschreibung | Der KDC-Proxyserverdienst wird auf Edgeservern ausgeführt, um als Proxy für Kerberos-Protokollnachrichten für Domänencontroller im Unternehmensnetzwerk zu fungieren. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

KtmRm für Distributed Transaction Coordinator

| | |
|------------|-------|
| | |
| Dienstname | KtmRm |

| | |
|---------------------|---|
| | |
| Beschreibung | Koordiniert Transaktionen zwischen dem Distributed Transaction Coordinator (MSDTC) und dem Kerneltransaktions-Manager (KTM). Wir empfehlen dir, diesen Dienst zu beenden, falls er nicht benötigt wird. Falls der Dienst benötigt wird, wird er sowohl vom MSDTC als auch vom KTM automatisch gestartet. Wenn dieser Dienst deaktiviert ist, tritt für alle MSDTC-Transaktionen, die mit einem Kernelressourcen-Manager interagieren, ein Fehler auf. Alle Dienste, die explizit davon abhängen, können nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Verbindungsschicht-Topologieerkennungszuordnungsprogramm

| | |
|---------------------|--|
| | |
| Dienstname | ltdsvc |
| Beschreibung | Erstellt eine Netzwerkübersicht mit Computer- und Gerätetopologieinformationen (d. h. Konnektivitätsinformationen) sowie Metadaten, die jeden PC und jedes Gerät beschreiben. Wenn dieser Dienst deaktiviert wird, funktioniert die Netzwerkübersicht nicht richtig. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | Kann deaktiviert werden, wenn keine Abhängigkeiten von der Netzwerkübersicht bestehen. |
| | |

Lokaler Sitzungs-Manager

| | |
|---------------------|---|
| | |
| Dienstname | LSM |
| Beschreibung | Windows-Kerndienst, der lokale Benutzersitzungen verwaltet. Das Beenden oder Deaktivieren dieses Diensts führt zu Instabilität des Systems. |
| Installation | Immer installiert |

| | |
|------------|--------------|
| | |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Standardsammlungsdienst des Microsoft(R)-Diagnose-Hubs

| | |
|--------------|---|
| | |
| Dienstname | diagnosticshub.standardcollector.service |
| Beschreibung | Standardsammlungsdienst des Diagnose-Hubs. Bei der Ausführung sammelt dieser Dienst ETW-Echtzeitereignisse und verarbeitet sie. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Anmelde-Assistent für Microsoft-Konten

| | |
|--------------|--|
| | |
| Dienstname | wlidsvc |
| Beschreibung | Ermöglicht die Benutzeranmeldung über die Identitätsdienste des Microsoft-Kontos. Wenn dieser Dienst beendet wird, können sich Benutzer nicht mehr mit ihrem Microsoft-Konto am Computer anmelden. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | Microsoft-Konten sind unter Windows Server nicht verfügbar. |
| | |

Microsoft App-V Client

| | |
|------------|------------|
| | |
| Dienstname | AppVClient |

| | |
|---------------------|---|
| | |
| Beschreibung | Dient zum Verwalten von App-V-Benutzern und virtuellen Anwendungen. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Deaktiviert |
| Empfehlung | Bereits deaktiviert |
| Kommentare | |
| | |

Microsoft iSCSI-Initiator-Dienst

| | |
|---------------------|---|
| | |
| Dienstname | MSiSCSI |
| Beschreibung | Dient zum Verwalten von iSCSI-Sitzungen (Internet SCSI) von diesem Computer zu iSCSI-Remotezielgeräten. Wenn dieser Dienst beendet wird, kann sich dieser Computer nicht an iSCSI-Zielen anmelden und nicht darauf zugreifen. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Unsere Diagnosedaten deuten darauf hin, dass dieser Dienst auf Clients und auf Servern genutzt wird. Die Deaktivierung hat keinerlei Vorteile. |
| | |

Microsoft Passport

| | |
|---------------------|---|
| | |
| Dienstname | NgcSvc |
| Beschreibung | Ermöglicht eine Prozessisolation für Kryptografieschlüssel, die zum Authentifizieren der zugeordneten Identitätsanbieter eines Benutzers verwendet werden. Wenn dieser Dienst deaktiviert wird, ist die gesamte Anwendung und Verwaltung dieser Schlüssel nicht verfügbar. Dies gilt auch für die Computeranmeldung und einmaliges Anmelden für Apps und Websites. Dieser Dienst wird automatisch gestartet und beendet. Wir empfehlen dir, diesen Dienst nicht neu zu konfigurieren. |
| Installation | Nur mit Desktopdarstellung |

| | |
|------------|---|
| | |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | Wird für PIN/Hello-Anmeldungen benötigt, die auf dem Server nicht unterstützt werden. |
| | |

Microsoft Passport-Container

| | |
|--------------|---|
| | |
| Dienstname | NgcCtnrSvc |
| Beschreibung | Verwaltet lokale Benutzeridentitätsschlüssel, um Benutzer für Identitätsanbieter und virtuelle TPM-Smartcards zu authentifizieren. Wenn dieser Dienst deaktiviert wird, kann nicht auf lokale Benutzeridentitätsschlüssel und virtuelle TPM-Smartcards zugegriffen werden. Wir empfehlen dir, diesen Dienst nicht neu zu konfigurieren. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | |
| | |

Microsoft-Softwareschattenkopie-Anbieter

| | |
|--------------|--|
| | |
| Dienstname | swprv |
| Beschreibung | Verwaltet softwarebasierte Volumeschattenkopien des Volumeschattenkopie-Diensts. Softwarebasierte Volumeschattenkopien können nicht verwaltet werden, wenn dieser Dienst beendet wird. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Microsoft-SMP für Speicherplätze

| | |
|--------------|--|
| | |
| Dienstname | smphost |
| Beschreibung | Hostdienst für den Microsoft-Verwaltungsanbieter für Speicherplätze. Wird dieser Dienst beendet oder deaktiviert, ist die Verwaltung von Speicherplätzen nicht mehr möglich. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Für APIs für die Speicherverwaltung tritt ohne diesen Dienst ein Fehler auf. Beispiel: "Get-WmiObject -class MSFT_Disk -Namespace Root\Microsoft\Windows\Storage". |
| | |

Net.Tcp-Portfreigabedienst

| | |
|--------------|---|
| | |
| Dienstname | NetTcpPortSharing |
| Beschreibung | Ermöglicht die Freigabe von TCP-Ports über das net.tcp-Protokoll. |
| Installation | Immer installiert |
| Starttyp | Deaktiviert |
| Empfehlung | Bereits deaktiviert |
| Kommentare | |
| | |

Netlogon

| | |
|--------------|--|
| | |
| Dienstname | Netlogon |
| Beschreibung | Dient zum Verwalten eines sicheren Kanals zwischen diesem Computer und dem Domänencontroller für die Authentifizierung von Benutzern und Diensten. Wenn dieser Dienst angehalten wird, kann der Computer Benutzer und Dienste möglicherweise nicht authentifizieren, und der Domänencontroller kann keine DNS-Datensätze registrieren. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |

| | |
|------------|--------------|
| | |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Netzwerkverbindungsbroker

| | |
|--------------|--|
| | |
| Dienstname | NcbService |
| Beschreibung | Fungiert als Broker für Verbindungen, über die Microsoft Store-Apps Benachrichtigungen über das Internet empfangen können. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | |
| | |

Netzwerkverbindungen

| | |
|--------------|--|
| | |
| Dienstname | Netman |
| Beschreibung | Verwaltet Objekte im Ordner „Netzwerk- und Wählverbindungen“, in dem LAN- und Remoteverbindungen angezeigt werden. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Netzwerkkonnektivitäts-Assistent

| | |
|------------|--------|
| | |
| Dienstname | NcaSvc |

| | |
|---------------------|--|
| | |
| Beschreibung | Stellt die Benachrichtigung zum DirectAccess-Status für Komponenten der Benutzeroberfläche bereit. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Netzwerklistendienst

| | |
|---------------------|--|
| | |
| Dienstname | netprofm |
| Beschreibung | Identifiziert die Netzwerke, mit denen der Computer eine Verbindung hergestellt hat, sammelt und speichert Eigenschaften für diese Netzwerke und benachrichtigt Anwendungen, wenn sich diese Eigenschaften ändern. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

NLA (Network Location Awareness)

| | |
|---------------------|--|
| | |
| Dienstname | NlaSvc |
| Beschreibung | Sammelt und speichert Konfigurationsinformationen für das Netzwerk und benachrichtigt Programme, wenn diese Informationen geändert werden. Wenn dieser Dienst beendet wird, sind die Konfigurationsinformationen möglicherweise nicht verfügbar. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |

| | |
|--|--|
| | |
| | |

Netzwerkeinrichtungsdienst

| | |
|--------------|--|
| | |
| Dienstname | NetSetupSvc |
| Beschreibung | Der Netzwerkeinrichtungsdienst verwaltet die Installation von Netzwerktreibern und ermöglicht die Konfiguration von Netzwerkeinstellungen auf unterer Ebene. Wenn der Dienst beendet wird, werden aktuell ausgeführte Treiberinstallationen unter Umständen abgebrochen. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Netzwerkspeicher-Schnittstellendienst

| | |
|--------------|---|
| | |
| Dienstname | nsi |
| Beschreibung | Dieser Dienst stellt Netzwerkbenachrichtigungen (z. B. beim Hinzufügen/Löschen von Schnittstellen) für Benutzermodusclients bereit. Wenn du diesen Dienst beendest, wird die Netzwerkkonnektivität getrennt. Wenn dieser Dienst deaktiviert wird, können andere Dienste, die von diesem Dienst ausschließlich abhängig sind, nicht mehr gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Offlinedateien

| | |
|------------|------------|
| | |
| Dienstname | CscService |

| | |
|---------------------|---|
| | |
| Beschreibung | Der Offlinedateiendienst führt Wartungsaktivitäten am Cache für Offlinedateien aus, reagiert auf Benutzeranmelde- und -abmeldeereignisse, implementiert die internen Komponenten der öffentlichen API, leitet interessante Ereignisse an Empfänger weiter, die an Offlineaktivitäten interessiert sind, und ändert den Cachestatus. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Deaktiviert |
| Empfehlung | Bereits deaktiviert |
| Kommentare | |
| | |

Laufwerke optimieren

| | |
|---------------------|--|
| | |
| Dienstname | defragsvc |
| Beschreibung | Unterstützt den Computer bei einer effizienteren Ausführung durch das Optimieren von Dateien auf Speicherlaufwerken. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Leistungsindikator-DLL-Host

| | |
|---------------------|--|
| | |
| Dienstname | PerfHost |
| Beschreibung | Ermöglicht Remotebenutzern und 64-Bit-Prozessen die Abfrage von Leistungsindikatoren, die von 32-Bit-DLLs bereitgestellt werden. Wenn dieser Dienst beendet wird, können nur lokale Benutzer und 32-Bit-Prozesse die von den 32-Bit-DLLs bereitgestellten Leistungsindikatoren abfragen. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |

| | |
|------------|--|
| | |
| Kommentare | |
| | |

Leistungsprotokolle und -warnungen

| | |
|--------------|--|
| | |
| Dienstname | pla |
| Beschreibung | „Leistungsprotokolle und -warnungen“ sammelt Leistungsdaten von lokalen oder Remotecomputern basierend auf vorkonfigurierten Zeitplanparametern und schreibt die Daten dann in ein Protokoll oder löst eine Warnung aus. Wenn dieser Dienst beendet wird, werden keine Leistungsinformationen erfasst. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Telefondienst

| | |
|--------------|---|
| | |
| Dienstname | PhoneSvc |
| Beschreibung | Verwaltet den Telefoniestatus des Geräts. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | Wird von modernen VoIP-Apps verwendet. |
| | |

Plug & Play

| | |
|------------|----------|
| | |
| Dienstname | PlugPlay |

| | |
|---------------------|--|
| | |
| Beschreibung | Ermöglicht einem Computer die Erkennung und Anpassung an Hardwareänderungen mit nur wenigen oder ganz ohne Benutzereingaben. Das Beenden oder Deaktivieren dieses Diensts führt zu Instabilität des Systems. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Enumeratordienst für tragbare Geräte

| | |
|---------------------|--|
| | |
| Dienstname | WPDBusEnum |
| Beschreibung | Erzwingt Gruppenrichtlinien für Wechsel-Massenspeichergeräte. Ermöglicht Anwendungen wie Windows Media Player und dem Bildimport-Assistenten, Inhalte unter Verwendung von Wechsel-Massenspeichergeräten zu übertragen und zu synchronisieren. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Leistung

| | |
|---------------------|--|
| | |
| Dienstname | Leistung |
| Beschreibung | Verwaltet die Energierichtlinie und die Zustellung der Energierichtlinienbenachrichtigung. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Druckspooler

| | |
|--------------|--|
| | |
| Dienstname | Spooler |
| Beschreibung | Dieser Dienst spoolt Druckaufträge und verarbeitet Interaktionen mit dem Drucker. Wenn du diesen Dienst ausschaltest, kannst du weder drucken noch Drucker anzeigen. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kann deaktiviert werden, wenn es sich nicht um einen Druckerserver oder einen Domänencontroller handelt. |
| Kommentare | <p>Auf einem Domänencontroller wird dem Spoolerdienst bei Installation der Domänencontroller-Rolle ein Thread hinzugefügt, der für die Durchführung der Druckbereinigung zuständig ist. Hiermit werden die veralteten Objekte der Druckwarteschlange aus Active Directory entfernt. Wenn der Spoolerdienst nicht auf mindestens einem DC auf jeder Site ausgeführt wird, kann AD keine alten Warteschlangen entfernen, die nicht mehr vorhanden sind.</p> <p>https://blogs.technet.microsoft.com/askperf/2008/11/18/disabling-unnecessary-services-a-word-to-the-wise/</p> |
| | |

Druckererweiterungen und Benachrichtigungen

| | |
|--------------|--|
| | |
| Dienstname | PrintNotify |
| Beschreibung | Mit diesem Dienst werden benutzerdefinierte Druckerdialogfelder geöffnet und Benachrichtigungen von einem Remotedruckerserver oder Drucker verarbeitet. Wenn du diesen Dienst deaktivierst, werden keine Druckererweiterungen oder Benachrichtigungen angezeigt. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kann deaktiviert werden, wenn es sich nicht um einen Druckerserver handelt. |
| Kommentare | |
| | |

Unterstützung in der Systemsteuerung unter Lösungen für Probleme

| | |
|------------|---------------|
| | |
| Dienstname | wercplsupport |

| | |
|---------------------|---|
| | |
| Beschreibung | Dieser Dienst bietet Unterstützung für das Anzeigen, Senden und Löschen von Problembereichen auf Systemebene für das Applet „Lösungen für Probleme“ in der Systemsteuerung. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Programmkompatibilitäts-Assistent-Dienst

| | |
|---------------------|--|
| | |
| Dienstname | PcaSvc |
| Beschreibung | Dieser Dienst bietet Unterstützung für den Programmkompatibilitäts-Assistenten (Program Compatibility Assistant, PCA). Mit dem PCA werden die vom Benutzer installierten und ausgeführten Programme überwacht. Wenn dieser Dienst beendet wird, wird der PCA nicht ordnungsgemäß ausgeführt. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Automatisch |
| Empfehlung | Deaktivierung OK |
| Kommentare | |
| | |

Verbessertes Windows-Audio-/Video-Streaming

| | |
|---------------------|---|
| | |
| Dienstname | QWAVE |
| Beschreibung | Der Windows-Dienst für verbessertes Audio/Video-Streaming (qWave) ist eine Netzwerkplattform für Audio/Video-Streaminganwendungen (AV) in privaten IP-Netzwerken. qWave verbessert die AV-Streamingleistung und -zuverlässigkeit, indem Netzwerk-QoS (Quality-of-Service) für AV-Anwendungen sichergestellt wird. Es werden Mechanismen für Zugangssteuerung, Laufzeitüberwachung und -erzwingung, Anwendungsfeedback sowie Verkehrspriorisierung bereitgestellt. |
| Installation | Nur mit Desktopdarstellung |

| | |
|------------|---------------------------|
| | |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | Clientseitiger QoS-Dienst |
| | |

Funkverwaltungsdienst

| | |
|--------------|---|
| | |
| Dienstname | RmSvc |
| Beschreibung | Dienst für Funkverwaltung und Flugzeugmodus |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | |
| | |

Verwaltung für automatische RAS-Verbindung

| | |
|--------------|--|
| | |
| Dienstname | RasAuto |
| Beschreibung | Erstellt eine Verbindung mit einem Remotenetzwerk, wenn ein Programm auf einen Remote-DNS- oder -NetBIOS-Namen (bzw. eine Adresse) verweist. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

RAS-Verbindungs-Manager

| | |
|------------|--------|
| | |
| Dienstname | RasMan |

| | |
|---------------------|--|
| | |
| Beschreibung | Verwaltet Einwähl- und VPN-Verbindungen zwischen diesem Computer und dem Internet oder anderen Remotenetzwerken. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Remotedesktopkonfiguration

| | |
|---------------------|---|
| | |
| Dienstname | SessionEnv |
| Beschreibung | Der Remotedesktop-Konfigurationsdienst (Remote Desktop Configuration Service, RDCS) ist für alle Konfigurations- und Sitzungsverwaltungsaktivitäten im Zusammenhang mit den Remotedesktopdiensten und Remotedesktop zuständig, die den SYSTEM-Kontext erfordern. Dazu gehören die sitzungsspezifischen temporären Ordner, Remotedesktopthemen und Remotedesktopzertifikate. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | |
| | |

Remotedesktopdienste

| | |
|---------------------|---|
| | |
| Dienstname | TermService |
| Beschreibung | Ermöglicht Benutzern das Herstellen einer interaktiven Verbindung mit einem Remotecomputer. Remotedesktop und Remotedesktop-Hostserver können nur zusammen mit diesem Dienst verwendet werden. Wenn du die Remoteverwendung dieses Computers verhindern möchtest, muss du die Kontrollkästchen auf der Registerkarte „Remote“ in den Systemsteuerungsoptionen deaktivieren. |
| Installation | Immer installiert |

| | |
|------------|--------------------|
| | |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | |
| | |

Anschlussumleitung für Remotedesktopdienst im Benutzermodus

| | |
|--------------|---|
| | |
| Dienstname | UmRdpService |
| Beschreibung | Ermöglicht die Umleitung von Druckern, Laufwerken und Anschlüssen für RDP-Verbindungen. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Unterstützt Umleitungen auf der Serverseite der Verbindung. |
| | |

Remoteprozeduraufruf (RPC)

| | |
|--------------|--|
| | |
| Dienstname | RpcSs |
| Beschreibung | Der RPCSS-Dienst wird als Dienststeuerungs-Manager für COM- und DCOM-Server verwendet. Von ihm werden Objektaktivierungsanforderungen, Objektexporterauflösungen und die verteilte Garbage Collection für COM- und DCOM-Server ausgeführt. Wenn dieser Dienst beendet oder deaktiviert wird, werden Programme, für die COM oder DCOM verwendet wird, nicht ordnungsgemäß ausgeführt. Wir empfehlen dir dringend, den RPCSS-Dienst auszuführen. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

RPC-Locator

| | |
|--------------|---|
| | |
| Dienstname | RpcLocator |
| Beschreibung | Unter Windows 2003 und früheren Windows-Versionen wird mit dem RPC-Locatordienst (Remote Procedure Call) die RPC-Namensdienstdatenbank verwaltet. Unter Windows Vista und höheren Windows-Versionen stellt dieser Dienst keine Funktionalität bereit und ist nur für Zwecke der Anwendungskompatibilität vorhanden. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Remoteregistrierung

| | |
|--------------|--|
| | |
| Dienstname | RemoteRegistry |
| Beschreibung | Ermöglicht es Remotebenutzern, Registrierungseinstellungen dieses Computers zu verändern. Wenn dieser Dienst beendet wird, kann die Registrierung nur von lokalen Benutzern dieses Computers verändert werden. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Nicht deaktivieren |
| Kommentare | |
| | |

Richtlinienergebnissatzanbieter

| | |
|--------------|---|
| | |
| Dienstname | RSoPProv |
| Beschreibung | Stellt einen Netzwerkdienst bereit, der Anforderungen zum Simulieren der Anwendung von Gruppenrichtlinieneinstellungen auf einen Zielbenutzer oder -computer in verschiedenen Situationen verarbeitet und einen sich daraus ergebenden Satz von Richtlinieneinstellungen berechnet. |

| | |
|--------------|-------------------|
| | |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Routing und RAS

| | |
|--------------|---|
| | |
| Dienstname | RemoteAccess |
| Beschreibung | Bietet Routingdienste in LAN- und WAN-Netzwerkumgebungen. |
| Installation | Immer installiert |
| Starttyp | Deaktiviert |
| Empfehlung | Bereits deaktiviert |
| Kommentare | Bereits deaktiviert |
| | |

RPC-Endpunktzuordnung

| | |
|--------------|---|
| | |
| Dienstname | RpcEptMapper |
| Beschreibung | Löst RPC-Schnittstellen-IDs für den Transport von Endpunkten auf. Wenn dieser Dienst angehalten oder deaktiviert wird, können Programme, für die Remoteprozeduraufruf-Dienste (Remote Procedure Call, RPC) verwendet werden, nicht ordnungsgemäß ausgeführt werden. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Sekundäre Anmeldung

| | |
|--------------|--|
| | |
| Dienstname | seclogon |
| Beschreibung | Aktiviert das Starten von Prozessen mit verschiedenen Anmeldeinformationen. Wenn dieser Dienst beendet wird, ist dieser Typ von Anmeldezugriff nicht mehr verfügbar. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

SSTP-Dienst

| | |
|--------------|--|
| | |
| Dienstname | SstpSvc |
| Beschreibung | Unterstützt SSTP (Secure Socket Tunneling-Protokoll), um über VPN eine Verbindung mit Remotecomputern herzustellen. Wenn dieser Dienst deaktiviert ist, können Benutzer SSTP nicht für den Zugriff auf Remoteserver verwenden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Wenn der Dienst deaktiviert wird, treten RRAS-Fehler auf. |
| | |

Sicherheitskonto-Manager

| | |
|--------------|--|
| | |
| Dienstname | SamSs |
| Beschreibung | Durch den Start dieses Diensts wird anderen Diensten signalisiert, dass die Sicherheitskontenverwaltung (SAM) bereit ist, Anforderungen anzunehmen. Wenn du diesen Dienst deaktivierst, wird verhindert, dass andere Dienste im System benachrichtigt werden, wenn die Sicherheitskontenverwaltung bereit ist. Dies kann wiederum dazu führen, dass diese Dienste nicht korrekt gestartet werden. Dieser Dienst sollte nicht deaktiviert werden. |
| Installation | Immer installiert |

| | |
|------------|--------------------|
| | |
| Starttyp | Automatisch |
| Empfehlung | Nicht deaktivieren |
| Kommentare | |
| | |

Sensordatendienst

| | |
|--------------|---|
| | |
| Dienstname | SensorDataService |
| Beschreibung | Liefert Daten von verschiedenen Sensoren. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | |
| | |

Sensorüberwachungsdienst

| | |
|--------------|--|
| | |
| Dienstname | SensrSvc |
| Beschreibung | Überwacht verschiedene Sensoren, um Daten verfügbar zu machen und eine Anpassung an den System- und Benutzerstatus vorzunehmen. Wird dieser Dienst beendet oder deaktiviert, wird die Anzeigehelligkeit nicht an die Lichtbedingungen der Umgebung angepasst. Das Beenden des Diensts kann auch andere Systemfeatures betreffen. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | |
| | |

Sensordienst

| | |
|------------|---------------|
| | |
| Dienstname | SensorService |

| | |
|---------------------|--|
| | |
| Beschreibung | Ein Sensordienst, der die Funktionen verschiedener Sensoren verwaltet. Er verwaltet SDO (Simple Device Orientation) und den Verlauf für Sensoren und lädt den SDO-Sensor, der Änderungen der Geräteausrichtung meldet. Wenn der Dienst beendet oder deaktiviert wird, wird der SDO-Sensor nicht geladen, und es findet keine automatische Drehung statt. Die Sammlung von Verlaufsdaten von den Sensoren wird ebenfalls beendet. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | |
| | |

Server

| | |
|---------------------|--|
| | |
| Dienstname | LanmanServer |
| Beschreibung | Unterstützt Datei-, Drucker- und Named-Piped-Freigabe für diesen Computer über das Netzwerk. Diese Funktionen sind nicht mehr verfügbar, falls dieser Dienst beendet wird. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Wird für die Remoteverwaltung, IPC\$ und SMB-Dateifreigabe benötigt. |
| | |

Shellhardwareerkennung

| | |
|---------------------|--|
| | |
| Dienstname | ShellHWDetection |
| Beschreibung | Zeigt Meldungen für Hardwareereignisse für automatische Wiedergabe an. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Automatisch |

| | |
|-------------------|------------------|
| | |
| Empfehlung | Deaktivierung OK |
| Kommentare | |
| | |

Smartcard

| | |
|---------------------|---|
| | |
| Dienstname | SCardSvr |
| Beschreibung | Verwaltet den Zugriff auf Smartcards, die von diesem Computer gelesen werden. Wenn dieser Dienst beendet wird, kann der Computer keine Smartcards mehr lesen. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Deaktiviert |
| Empfehlung | Bereits deaktiviert |
| Kommentare | |
| | |

Smartcard-Geräteaufzählungsdienst

| | |
|---------------------|--|
| | |
| Dienstname | ScDeviceEnum |
| Beschreibung | Erstellt Softwaregeräteknotten für alle Smartcardleser, die einer bestimmten Sitzung zur Verfügung stehen. Wird dieser Dienst deaktiviert, können von WinRT-APIs keine Smartcardleser aufgezählt werden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | Wird fast ausschließlich für WinRT-Apps benötigt. |
| | |

Richtlinie zum Entfernen der Smartcard

| | |
|-------------------|-------------|
| | |
| Dienstname | SCPolicySvc |

| | |
|---------------------|--|
| | |
| Beschreibung | Lässt eine Konfiguration des Systems zu, bei der der Benutzerdesktop beim Entfernen der Smartcard gesperrt wird. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

SNMP-Trap

| | |
|---------------------|--|
| | |
| Dienstname | SNMPTRAP |
| Beschreibung | Empfängt Trap-Nachrichten, die von lokalen oder Remote-SNMP-Agents generiert wurden, und leitet die Nachrichten an SNMP-Verwaltungsprogramme weiter, die auf diesem Computer ausgeführt werden. SNMP-basierte Programme auf diesem Computer empfangen keine SNMP-Trap-Nachrichten, falls dieser Dienst beendet wird. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Softwareschutz

| | |
|---------------------|--|
| | |
| Dienstname | sppsvc |
| Beschreibung | Aktiviert das Herunterladen, die Installation und die Durchsetzung digitaler Lizenzen für Windows und Windows-Anwendungen. Wenn der Dienst deaktiviert wird, werden das Betriebssystem und lizenzierte Anwendungen in einem Benachrichtigungsmodus ausgeführt. Es wird dringend empfohlen, den Softwareschutzdienst nicht zu deaktivieren. |
| Installation | Immer installiert |
| Starttyp | Automatisch |

| | |
|-------------------|--------------|
| | |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Hilfsprogramm für spezielle Verwaltungskonsole

| | |
|---------------------|--|
| | |
| Dienstname | sacsvr |
| Beschreibung | Ermöglicht Administratoren über die Notverwaltungsdienste (Emergency Management Services, EMS) den Remotezugriff auf eine Eingabeaufforderung. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Echtzeit-Datenträgerprüfung

| | |
|---------------------|---|
| | |
| Dienstname | svsvc |
| Beschreibung | Überprüft mögliche Beschädigungen des Dateisystems. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

SSDP-Suche

| | |
|-------------------|---------|
| | |
| Dienstname | SSDPSRV |

| | |
|---------------------|--|
| | |
| Beschreibung | Sucht nach Netzwerkgeräten und -diensten, die das SSDP-Suchprotokoll verwenden, z. B. UPnP-Geräte. Kündigt zudem SSDP-Geräte und -dienste an, die auf dem lokalen Computer ausgeführt werden. Wenn dieser Dienst beendet wird, werden SSDP-basierte Geräte nicht entdeckt. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | |
| | |

StateRepository-Dienst

| | |
|---------------------|---|
| | |
| Dienstname | StateRepository |
| Beschreibung | Bietet die erforderliche Infrastrukturunterstützung für das Anwendungsmodell. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Ereignisse zum Abrufen von Standbildern

| | |
|---------------------|---|
| | |
| Dienstname | WiaRpc |
| Beschreibung | Startet Anwendungen im Zusammenhang mit Ereignissen zum Abrufen von Standbildern. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | |
| | |

Speicherdienst

| | |
|--------------|--|
| | |
| Dienstname | StorSvc |
| Beschreibung | Stellt Unterstützungsdienste für Speichereinstellungen und externe Speichererweiterung bereit. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Storage Tiers Management

| | |
|--------------|---|
| | |
| Dienstname | TieringEngineService |
| Beschreibung | Optimiert die Verteilung der Daten auf den Speicherstufen für alle mehrstufigen Speicherplätze im System. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Superfetch

| | |
|--------------|--|
| | |
| Dienstname | SysMain |
| Beschreibung | Verwaltet und verbessert die Systemleistung im Zeitablauf. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Synchronisierungshost

| | |
|--------------|---|
| | |
| Dienstname | OneSyncSvc |
| Beschreibung | Dieser Dienst synchronisiert E-Mail-, Kontakt-, Kalender- und verschiedene andere Benutzerdaten. Wenn dieser Dienst nicht ausgeführt wird, funktionieren E-Mail-Programme und andere Anwendungen, die von dieser Funktionalität abhängig sind, nicht ordnungsgemäß. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Automatisch |
| Empfehlung | Deaktivierung OK |
| Kommentare | Benutzerdienstvorlage |
| | |

Benachrichtigungsdienst für Systemereignisse

| | |
|--------------|---|
| | |
| Dienstname | SENS |
| Beschreibung | Überwacht Systemereignisse und benachrichtigt Abonnenten des COM+-Ereignissystems bei diesen Ereignissen. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Systemereignissebroker

| | |
|--------------|--|
| | |
| Dienstname | SystemEventsBroker |
| Beschreibung | Koordiniert die Ausführung der Hintergrundvorgänge für WinRT-Anwendungen. Wird dieser Dienst beendet oder deaktiviert, werden die Hintergrundvorgänge unter Umständen nicht ausgelöst. |
| Installation | Immer installiert |
| Starttyp | Automatisch |

| | |
|-------------------|--|
| | |
| Empfehlung | Nicht deaktivieren |
| Kommentare | In der Beschreibung wird nur die Nutzung für WinRT-Apps erwähnt, aber der Dienst wird auch für die Aufgabenplanung, den Brokerinfrastrukturdienst und andere interne Komponenten benötigt. |
| | |

Aufgabenplanung

| | |
|---------------------|---|
| | |
| Dienstname | Zeitplan |
| Beschreibung | Ermöglicht es einem Benutzer, automatische Aufgaben auf diesem Computer zu konfigurieren und zu planen. Der Dienst hostet auch mehrere kritische Aufgaben für das Windows-System. Wenn dieser Dienst beendet oder deaktiviert wird, werden diese Vorgänge nicht zu den geplanten Zeiten ausgeführt. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

TCP/IP-NetBIOS-Hilfsdienst

| | |
|---------------------|--|
| | |
| Dienstname | lmhosts |
| Beschreibung | Bietet Unterstützung für den NetBIOS-über-TCP/IP-Dienst (NetBT) und die NetBIOS-Namensauflösung für Clients im Netzwerk, sodass Benutzer Daten gemeinsam nutzen, drucken und sich am Netzwerk anmelden können. Diese Funktionen sind nicht mehr verfügbar, falls dieser Dienst beendet wird. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Telephony

| | |
|--------------|---|
| | |
| Dienstname | TapiSrv |
| Beschreibung | Bietet Telefonie-API-Unterstützung (TAPI) für Programme, die lokale und über das LAN auf Servern (die diesen Dienst ebenfalls ausführen) angebundene Telefoniegeräte steuern. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Wenn der Dienst deaktiviert wird, treten RRAS-Fehler auf. |
| | |

Designs

| | |
|--------------|---|
| | |
| Dienstname | Designs |
| Beschreibung | Stellt die Designverwaltung zur Verfügung. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Automatisch |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Es können keine Designs für Barrierefreiheit festgelegt werden, wenn dieser Dienst deaktiviert ist. |
| | |

Kacheldaten-Modellserver

| | |
|--------------|--|
| | |
| Dienstname | tiledatamodelsvc |
| Beschreibung | Kachelserver zur Kachelaktualisierung. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Automatisch |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Wenn dieser Dienst deaktiviert wird, tritt für das Startmenü ein Fehler auf. |

| | |
|--|--|
| | |
| | |

Zeitbroker

| | |
|--------------|--|
| | |
| Dienstname | TimeBrokerSvc |
| Beschreibung | Koordiniert die Ausführung der Hintergrundvorgänge für WinRT-Anwendungen. Wird dieser Dienst beendet oder deaktiviert, werden die Hintergrundvorgänge unter Umständen nicht ausgelöst. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | In der Beschreibung wird nur die Nutzung für WinRT-Apps erwähnt, aber der Dienst wird auch für die Aufgabenplanung, den Brokerinfrastrukturdienst und andere interne Komponenten benötigt. |
| | |

Dienst für Bildschirmstatur und Schreibbereich

| | |
|--------------|---|
| | |
| Dienstname | TabletInputService |
| Beschreibung | Aktiviert die Stift- und Freihandfunktionalität der Bildschirmstatur und des Schreibbereichs. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | |
| | |

Update Orchestrator Service für Windows Update

| | |
|--------------|--|
| | |
| Dienstname | UsoSvc |
| Beschreibung | Verwaltet Windows-Updates. Wenn der Dienst beendet wird, können auf deinen Geräten keine aktuellen Updates heruntergeladen und installiert werden. |

| | |
|--------------|---|
| | |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | In v1607 hat die Dienstbeschreibung gefehlt. Dieser Dienst wird für Windows Update (inkl. WSUS) benötigt. |
| | |

UPnP-Gerätehost

| | |
|--------------|---|
| | |
| Dienstname | upnphost |
| Beschreibung | Ermöglicht es, dass UPnP-Geräte auf diesem Computer gehostet werden können. Wenn dieser Dienst beendet wird, sind alle gehosteten UPnP-Geräte nicht mehr betriebsbereit, und es können keine weiteren gehosteten Geräte hinzugefügt werden. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | |
| | |

Dienst für die Benutzerzugriffsprotokollierung

| | |
|------------|--------|
| | |
| Dienstname | UALSVC |

| | |
|---------------------|--|
| | |
| Beschreibung | Mithilfe dieses Diensts werden eindeutige Clientzugriffsanforderungen in Form von IP-Adressen und Benutzernamen von auf dem lokalen Server installierten Produkten und Rollen protokolliert. Diese Informationen können über PowerShell von Administratoren abgefragt werden, die den Clientbedarf an Serversoftware für die Offlineverwaltung von Clientzugriffslizenzen (Client Access License, CAL) berechnen müssen. Wenn der Dienst deaktiviert wird, werden Clientanforderungen nicht protokolliert und sind daher nicht über PowerShell-Abfragen abrufbar. Wird der Dienst beendet, so beeinflusst dies nicht die Abfrage von Verlaufsdaten. (Schritte zum Löschen von Verlaufsdaten findest du in der begleitenden Dokumentation.) Der lokale Systemadministrator muss in den Windows Server-Lizenzbedingungen die Anzahl von Clientzugriffslizenzen festlegen, die für eine ordnungsgemäße Lizenzierung der Serversoftware erforderlich ist. Die Verwendung des UAL-Diensts und der UAL-Daten entbinden nicht von dieser Verpflichtung. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Benutzerdatenzugriff

| | |
|---------------------|---|
| | |
| Dienstname | UserDataSvc |
| Beschreibung | Ermöglicht Apps den Zugriff auf strukturierte Benutzerdaten, z. B. Kontaktinformationen, Kalender, Nachrichten und andere Inhalte. Wenn du diesen Dienst beendest oder deaktivierst, funktionieren Apps, die diese Daten verwenden, möglicherweise nicht ordnungsgemäß. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | Benutzerdienstvorlage |
| | |

Benutzerdatenspeicher

| | |
|--------------|--|
| | |
| Dienstname | UnistoreSvc |
| Beschreibung | Verarbeitet die Speicherung strukturierter Benutzerdaten, z. B. Kontaktinformationen, Kalender, Nachrichten und andere Inhalte. Wenn du diesen Dienst beendest oder deaktivierst, funktionieren Apps, die diese Daten verwenden, möglicherweise nicht ordnungsgemäß. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | Benutzerdienstvorlage |
| | |

User Experience Virtualization-Dienst

| | |
|--------------|--|
| | |
| Dienstname | UevAgentService |
| Beschreibung | Stellt Unterstützung für das Roaming von Anwendungen und Betriebssystemeinstellungen bereit. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Deaktiviert |
| Empfehlung | Bereits deaktiviert |
| Kommentare | |
| | |

Benutzer-Manager

| | |
|--------------|---|
| | |
| Dienstname | UserManager |
| Beschreibung | Der Benutzer-Manager stellt die Laufzeitkomponenten bereit, die für Interaktionen mit mehreren Benutzern erforderlich sind. Wenn dieser Dienst beendet wird, funktionieren einige Anwendungen möglicherweise nicht korrekt. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |

| | |
|-------------------|--|
| | |
| Kommentare | |
| | |

Benutzerprofildienst

| | |
|---------------------|---|
| | |
| Dienstname | ProfSvc |
| Beschreibung | Dieser Dienst ist für das Laden und Entladen von Benutzerprofilen verantwortlich. Wenn dieser Dienst beendet oder deaktiviert ist, können Benutzer sich nicht mehr an- oder abmelden. Zudem können Probleme beim Abrufen von Benutzerdaten für Apps auftreten, und Komponenten, die für den Empfang von Profilereignisbenachrichtigungen registriert sind, erhalten keine Benachrichtigungen. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Virtueller Datenträger

| | |
|---------------------|---|
| | |
| Dienstname | vds |
| Beschreibung | Stellt Verwaltungsdienste für Datenträger, Volumes, Dateisysteme und Speicherarrays bereit. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Volumeschattenkopie

| | |
|-------------------|-----|
| | |
| Dienstname | VSS |

| | |
|---------------------|---|
| | |
| Beschreibung | Verwaltet und implementiert Volumeschattenkopien, die zu Sicherungs- und anderen Zwecken verwendet werden. Wenn dieser Dienst beendet wird, sind keine Schattenkopien für Sicherungen verfügbar, und die Sicherung kann eventuell fehlschlagen. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

WalletService

| | |
|---------------------|--|
| | |
| Dienstname | WalletService |
| Beschreibung | Von Clients der Funktion „Brieftasche“ verwendete Hostobjekte. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | |
| | |

Windows-Audio

| | |
|---------------------|---|
| | |
| Dienstname | Audiosrv |
| Beschreibung | Verwaltet Audioinhalte für Windows-basierte Programme. Wenn dieser Dienst beendet wird, funktionieren Audiogeräte und -effekte nicht ordnungsgemäß. Wenn der Dienst deaktiviert wird, können Dienste, die explizit von diesem Dienst abhängig sind, nicht gestartet werden. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |

| | |
|------------|--|
| | |
| Kommentare | |
| | |

Windows-Audio-Endpunkterstellung

| | |
|--------------|---|
| | |
| Dienstname | AudioEndpointBuilder |
| Beschreibung | Verwaltet Audiogeräte für den Windows-Audiodienst. Wenn dieser Dienst beendet wird, funktionieren Audiogeräte und -effekte nicht ordnungsgemäß. Wenn der Dienst deaktiviert wird, können Dienste, die explizit von diesem Dienst abhängig sind, nicht gestartet werden. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | |
| | |

Windows-Biometriedienst

| | |
|--------------|--|
| | |
| Dienstname | WbioSrv |
| Beschreibung | Mit dem Windows-Biometriedienst können in Clientanwendungen biometrische Daten erfasst, verglichen, geändert und gespeichert werden, ohne dass ein direkter Zugriff auf biometrische Hardware oder Proben erfolgt. Der Dienst wird in einem privilegierten SVCHOST-Prozess gehostet. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Windows-Kamera-FrameServer

| | |
|------------|-------------|
| | |
| Dienstname | FrameServer |

| | |
|---------------------|--|
| | |
| Beschreibung | Ermöglicht mehreren Clients den Zugriff auf Videoframes von Kameras. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | |
| | |

Windows-Verbindungs-Manager

| | |
|---------------------|---|
| | |
| Dienstname | Wcmsvc |
| Beschreibung | Anhand der aktuell auf dem PC verfügbaren Netzwerkkonnektivitätsoptionen wird die Verbindung automatisch hergestellt oder getrennt. Zudem kann die Netzwerkkonnektivität mithilfe von Gruppenrichtlinieneinstellungen verwaltet werden. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Windows Defender-Netzwerkinspektionsdienst

| | |
|---------------------|--|
| | |
| Dienstname | WdNisSvc |
| Beschreibung | Schützt gegen Eindringversuche bei bekannten und neu erkannten Sicherheitsrisiken von Netzwerkprotokollen. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Windows Defender-Dienst

| | |
|--------------|--|
| | |
| Dienstname | WinDefend |
| Beschreibung | Schützt Benutzer vor Schadsoftware und weiterer potenziell unerwünschter Software. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Windows Driver Foundation – Benutzermodus-Treiberframework

| | |
|--------------|---|
| | |
| Dienstname | wudfsvc |
| Beschreibung | Erstellt und verwaltet Benutzermodus-Treiberprozesse. Der Dienst kann nicht beendet werden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Hostdienst für Windows Encryption Provider

| | |
|--------------|--|
| | |
| Dienstname | WEPHOSTSVC |
| Beschreibung | Der Hostdienst für Windows Encryption Provider vermittelt Verschlüsselungsfunktionen von Drittanbieter-Verschlüsselungsanbietern an Prozesse, die EAS-Richtlinien bewerten und anwenden müssen. Wenn dieser Dienst beendet wird, sind die EAS-Kompatibilitätsüberprüfungen gefährdet, die von den verbundenen E-Mail-Konten eingerichtet wurden. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |

| | |
|-------------------|--------------|
| | |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Windows-Fehlerberichterstattungsdienst

| | |
|---------------------|--|
| | |
| Dienstname | WerSvc |
| Beschreibung | Ermöglicht die Berichterstattung von Fehlern bei nicht mehr funktionierenden und reagierenden Programmen und das Angeben von Lösungen. Ermöglicht außerdem das Generieren von Protokollen für Diagnose- und Reparaturdienste. Wenn dieser Dienst beendet wird, funktioniert die Fehlerberichterstattung möglicherweise nicht ordnungsgemäß, und die Ergebnisse von Diagnosediensten und Reparaturen werden möglicherweise nicht angezeigt. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Erfasst und sendet Daten zu Abstürzen und zum Hängen, die sowohl von MS als auch von Dritten (ISVs/IHVs) genutzt werden. Die Daten werden zum Diagnostizieren von Fehlern verwendet, die zu Abstürzen führen können. Dies können auch Sicherheitsfehler sein. Wird auch für die Fehlerberichterstattung in Unternehmen benötigt. |
| | |

Windows-Ereignissammlung

| | |
|---------------------|--|
| | |
| Dienstname | Wecsvc |
| Beschreibung | Dieser Dienst verwaltet permanente Abonnements für Ereignisse von Remotequellen, die das WS-Verwaltungsprotokoll unterstützen. Hierzu gehören Windows Vista-Ereignisprotokolle sowie Hardware- und IPMI-fähige Ereignisquellen. Der Dienst speichert weitergeleitete Ereignisse in einem lokalen Ereignisprotokoll. Falls dieser Dienst beendet oder deaktiviert wird, können Ereignisabonnements nicht erstellt und weitergeleitete Ereignisse nicht angenommen werden. |
| Installation | Immer installiert |
| Starttyp | Manuell |

| | |
|-------------------|--|
| | |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Erfasst ETW-Ereignisse (z. B. Sicherheitsereignisse) für Verwaltungs- und Diagnosezwecke. Von diesem Dienst sind viele Features und Drittanbietertools abhängig, z. B. Tools für die Sicherheitsüberwachung. |
| | |

Windows-Ereignisprotokoll

| | |
|---------------------|---|
| | |
| Dienstname | EventLog |
| Beschreibung | Dieser Dienst verwaltet Ereignisse und Ereignisprotokolle. Er unterstützt die Protokollierung, die Abfrage und das Abonnement von Ereignissen sowie die Archivierung von Ereignisprotokollen und die Verwaltung von Ereignismetadaten. Er kann Ereignisse im XML- und Nur-Text-Format anzeigen. Durch das Beenden dieses Diensts können die Sicherheit und Zuverlässigkeit des Systems beeinträchtigt werden. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Windows-Firewall

| | |
|---------------------|--|
| | |
| Dienstname | MpsSvc |
| Beschreibung | Die Windows-Firewall trägt zum Schutz des Computers bei, indem der Zugriff durch nicht autorisierte Benutzer auf den Computer über das Internet bzw. ein Netzwerk verhindert wird. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Windows-Dienst für Schriftartencache

| | |
|--------------|--|
| | |
| Dienstname | FontCache |
| Beschreibung | Optimiert die Leistung von Anwendungen durch das Speichern häufig verwendeter Schriftartendaten. Dieser Dienst wird von Anwendungen gestartet, wenn er nicht bereits ausgeführt wird. Er kann deaktiviert werden, aber dadurch wird die Leistung von Anwendungen herabgesetzt. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Windows-Bilderfassung (WIA)

| | |
|--------------|---|
| | |
| Dienstname | stisvc |
| Beschreibung | Stellt Bilderfassungsdienste für Scanner und Kameras zur Verfügung. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | |
| | |

Windows-Insider-Dienst

| | |
|--------------|-------------------|
| | |
| Dienstname | wisvc |
| Beschreibung | wisvc |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |

| | |
|-------------------|---|
| | |
| Kommentare | Für Server wird das Test-Flighting nicht unterstützt, sodass darauf kein Vorgang durchgeführt wird. Das Feature kann auch per Gruppenrichtlinie deaktiviert werden. |
| | |

Windows Installer

| | |
|---------------------|---|
| | |
| Dienstname | msiserver |
| Beschreibung | Fügt Anwendungen, die als Windows Installer-Paket (*.msi, *.msp) angeboten werden, hinzu bzw. ändert oder entfernt sie. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Windows-Lizenz-Manager-Dienst

| | |
|---------------------|--|
| | |
| Dienstname | LicenseManager |
| Beschreibung | Stellt Infrastrukturunterstützung für den Microsoft Store bereit. Der Dienst wird bei Bedarf gestartet, und bei einer Deaktivierung verhalten sich im Windows Store erworbene Inhalte nicht ordnungsgemäß. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Windows-Verwaltungsinstrumentation

| | |
|-------------------|---------|
| | |
| Dienstname | Winmgmt |

| | |
|---------------------|---|
| | |
| Beschreibung | Bietet eine standardmäßige Schnittstelle und ein Objektmodell zum Zugreifen auf Verwaltungsinformationen über das Betriebssystem, Geräte, Anwendungen und Dienste. Die meiste Windows-basierte Software kann nicht ordnungsgemäß ausgeführt werden, falls dieser Dienst beendet wird. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Windows-Dienst für mobile Hotspots

| | |
|---------------------|--|
| | |
| Dienstname | icssvc |
| Beschreibung | Ermöglicht die Freigabe einer Datenverbindung für ein anderes Gerät. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | |
| | |

Windows Modules Installer

| | |
|---------------------|--|
| | |
| Dienstname | TrustedInstaller |
| Beschreibung | Ermöglicht das Installieren, Ändern und Entfernen von Windows-Updates und optionalen Komponenten. Wenn dieser Dienst deaktiviert ist, können beim Installieren oder Deinstallieren von Windows-Updates auf diesem Computer Fehler auftreten. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |

| | |
|-------------------|--|
| | |
| Kommentare | |
| | |

Windows-Pushbenachrichtigungssystemdienst

| | |
|---------------------|--|
| | |
| Dienstname | WpnService |
| Beschreibung | Der Dienst wird in Sitzung 0 ausgeführt und hostet die Benachrichtigungsplattform und den Verbindungsanbieter, der die Verbindung zwischen Gerät und WNS-Server behandelt. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Automatisch |
| Empfehlung | Deaktivierung OK |
| Kommentare | Wird für Live-Kacheln und andere Features benötigt. |
| | |

Windows-Pushbenachrichtigungs-Benutzerdienst

| | |
|---------------------|---|
| | |
| Dienstname | WpnUserService |
| Beschreibung | Dieser Dienst hostet die Windows-Benachrichtigungsplattform, die lokale Benachrichtigungen und Pushbenachrichtigungen unterstützt. Unterstützt werden Kachel-, Popup- und unformatierte Benachrichtigungen. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung OK |
| Kommentare | Benutzerdienstvorlage |
| | |

Windows-Remoteverwaltung (WS-Verwaltung)

| | |
|-------------------|-------|
| | |
| Dienstname | WinRM |

| | |
|---------------------|---|
| | |
| Beschreibung | <p>Mit dem Windows-Remoteverwaltungsdienst (WinRM) wird das WS-Verwaltungsprotokoll für die Remoteverwaltung implementiert. Die WS-Verwaltung stellt ein Standard-Webdienst-Protokoll dar, das für die Remote-Software- und Hardware-Verwaltung verwendet wird. Der WinRM-Dienst durchsucht das Netzwerk nach WS-Verwaltungsanforderungen und verarbeitet diese. Der WinRM-Dienst muss mit einem „Listener“ unter Verwendung des Befehlszeilenprogramms winrm.cmd oder über die Gruppenrichtlinie konfiguriert werden, um im Netzwerk „lauschen“ zu können. Der WinRM-Dienst stellt einen Zugriff auf WMI-Daten bereit und ermöglicht eine Ereignissammlung. Die Ereignissammlung und das Abonnieren von Ereignissen machen es erforderlich, dass der Dienst ausgeführt wird. WinRM-Nachrichten verwenden HTTP oder HTTPS als Transporte. Der WinRM-Dienst ist nicht von IIS abhängig, er wird jedoch vorkonfiguriert, um auf demselben Computer einen Port mit IIS zu teilen. Der WinRM-Dienst reserviert das URL-Präfix „/wsman“. Um Konflikten mit IIS vorzubeugen, sollten Administratoren sicherstellen, dass keine auf IIS gehostete Website das URL-Präfix „/wsman“ verwendet.</p> |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Wird für die Remoteverwaltung benötigt. |
| | |

Windows Search

| | |
|---------------------|---|
| | |
| Dienstname | WSearch |
| Beschreibung | <p>Stellt Inhaltsindizierung, Eigenschaftenzwischenspeicherung und Suchergebnisse für Dateien, E-Mails und andere Inhalte bereit.</p> |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Deaktiviert |
| Empfehlung | Bereits deaktiviert |
| Kommentare | |
| | |

Windows-Zeitdienst

| | |
|--------------|--|
| | |
| Dienstname | W32Time |
| Beschreibung | Behält Datums- und Zeitsynchronisation auf allen Clients und Servern im Netzwerk bei. Wenn dieser Dienst beendet wurde, sind Zeit- und Datumssynchronisierung nicht verfügbar. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Windows Update

| | |
|--------------|---|
| | |
| Dienstname | wuauerv |
| Beschreibung | Erkennung, Download und Installation von Updates für Windows und andere Programme. Wenn der Dienst deaktiviert ist, können „Windows Update“ bzw. das Feature „Automatische Updates“ nicht verwendet werden. Außerdem können Programme dann die Windows Update-Agent-Anwendungsprogrammierschnittstelle (WUA API) nicht verwenden. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

WinHTTP-Web Proxy Auto-Discovery-Dienst

| | |
|--------------|---|
| | |
| Dienstname | WinHttpAutoProxySvc |
| Beschreibung | WinHTTP implementiert den HTTP-Clientstapel und bietet Entwicklern eine Win32-API und COM-Automatisierungskomponente zum Senden von HTTP-Anforderungen und zum Empfangen von Antworten. Außerdem unterstützt WinHTTP die automatische Erkennung von Proxykonfigurationen über die entsprechende Implementierung des WPAD-Protokolls (Web Proxy Auto-Discovery). |

| | |
|--|--|
| | |
|--|--|

| | |
|--------------|---|
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Nicht deaktivieren |
| Kommentare | Alle Elemente, die den Netzwerkstapel nutzen, können über eine funktionale Abhängigkeit von diesem Dienst verfügen. Er wird von vielen Organisationen genutzt, um das Routing von HTTP-Proxys für interne Netzwerke zu konfigurieren. Ohne diesen Dienst tritt für alle HTTP-Internetverbindungen mit internem Ursprung ein Fehler auf. |
| | |

Automatische Konfiguration (verkabelt)

| | |
|--------------|--|
| | |
| Dienstname | dot3svc |
| Beschreibung | Mit dem Dienst für die automatische Konfiguration von Kabelnetzwerken (DOT3SVC) wird eine IEEE 802.1X-Authentifizierung an Ethernet-Schnittstellen ausgeführt. Wenn bei der aktuellen verkabelten Netzwerkbereitstellung die 802.1X-Authentifizierung erzwungen wird, muss der DOT3SVC-Dienst so konfiguriert werden, dass eine Konnektivität auf der 2. Schicht hergestellt bzw. Zugriff auf Netzwerkressourcen ermöglicht wird. Der DOT3SVC-Dienst wirkt sich nicht auf Kabelnetzwerke aus, bei denen die 802.1X-Authentifizierung nicht erzwungen wird. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

WMI-Leistungsadapter

| | |
|------------|----------|
| | |
| Dienstname | wmiApSrv |

| | |
|---------------------|---|
| | |
| Beschreibung | Bietet Leistungsbibliotheksinformationen der Windows-Verwaltungsinstrumentationsanbieter für Clients im Netzwerk. Dieser Dienst wird nur ausgeführt, wenn das Leistungsdaten-Hilfsprogramm aktiviert ist. |
| Installation | Immer installiert |
| Starttyp | Manuell |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Arbeitsstation

| | |
|---------------------|---|
| | |
| Dienstname | LanmanWorkstation |
| Beschreibung | Erstellt und wartet Clientnetzwerkverbindungen mit Remoteservern unter Verwendung des SMB-Protokolls. Diese Verbindungen sind nicht mehr verfügbar, falls dieser Dienst beendet wird. Wenn dieser Dienst deaktiviert ist, können alle Dienste, die explizit davon abhängen, nicht gestartet werden. |
| Installation | Immer installiert |
| Starttyp | Automatisch |
| Empfehlung | Kein Hinweis |
| Kommentare | |
| | |

Xbox Live Authentifizierungs-Manager

| | |
|---------------------|---|
| | |
| Dienstname | XblAuthManager |
| Beschreibung | Stellt Authentifizierungs- und Autorisierungsservices für Xbox Live bereit. Wenn dieser Dienst beendet wird, funktionieren einige Anwendungen möglicherweise nicht korrekt. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung empfohlen |
| Kommentare | |

| | |
|--|--|
| | |
| | |

Xbox Live-Spiele speichern

| | |
|---------------------|---|
| | |
| Dienstname | XblGameSave |
| Beschreibung | Dieser Dienst synchronisiert für Xbox Live-Spiele gespeicherte Daten. Wenn der Dienst beendet wird, werden die gespeicherten Spieldaten für Xbox Live nicht hochgeladen bzw. heruntergeladen. |
| Installation | Nur mit Desktopdarstellung |
| Starttyp | Manuell |
| Empfehlung | Deaktivierung empfohlen |
| Kommentare | Dieser Dienst synchronisiert für Xbox Live-Spiele gespeicherte Daten. Wenn der Dienst beendet wird, werden die gespeicherten Spieldaten für Xbox Live nicht hochgeladen bzw. heruntergeladen. |
| | |

Windows-Authentifizierung: Übersicht

09.04.2020 • 10 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Navigationsthema für IT-Experten sind Dokumentationsressourcen für Technologien zur Windows-Authentifizierung und -Anmeldung aufgeführt, die Produktbewertungen, "Erste Schritte"-Handbücher, Verfahren, Entwurfs- und Bereitstellungshandbücher, technische Referenzen und Befehlsverzeichnisse enthalten.

Featurebeschreibung

Authentifizierung ist der Vorgang, durch den die Identität eines Objekts, eines Dienstes oder einer Person überprüft wird. Ziel der Authentifizierung eines Objekts ist es, sicherzustellen, dass das Objekt echt und unverfälscht ist. Beim Authentifizieren eines Diensts oder einer Person ist das Ziel, sicherzustellen, dass die vorgelegten Anmeldeinformationen authentisch sind.

Im Netzwerkkontext dient die Authentifizierung dazu, die Identität gegenüber einer Netzwerkanwendung oder -ressource nachzuweisen. In der Regel wird die Identität durch einen kryptografischen Vorgang nachgewiesen, der entweder einen Schlüssel verwendet, der nur dem Benutzer bekannt ist, und zwar mit Kryptografie mit öffentlichem Schlüssel oder einem gemeinsam genutzten Schlüssel. Auf der Serverseite der Authentifizierungskommunikation werden die signierten Daten mit einem bekannten Kryptografieschlüssel verglichen, um den Authentifizierungsversuch zu überprüfen.

Durch die Speicherung der Kryptografieschlüssel an einem zentralen Ort wird der Authentifizierungsvorgang skalierbar und verwaltbar. Active Directory Domain Services ist die empfohlene und Standardtechnologie für das Speichern von Identitätsinformationen (einschließlich der Kryptografieschlüssel, die die Anmelde Informationen des Benutzers) sind. Active Directory ist für Standardimplementierungen von Kerberos und NTLM erforderlich.

Authentifizierungstechniken reichen von einer einfachen Anmeldung, bei der Benutzer auf der Grundlage von etwas, das nur dem Benutzer bekannt ist, für leistungsfähigere Sicherheitsmechanismen identifiziert werden, die Benutzer wie Token, öffentliche Schlüssel Zertifikate und Biometrie verwenden. In einer Unternehmensumgebung ist es Diensten oder Benutzern eventuell möglich, auf unterschiedliche Anwendungen oder Ressourcen auf verschiedenen Arten von Servern an einem einzigen Standort oder auch standortübergreifend zugreifen. Aus diesem Grund muss die Authentifizierung Umgebungen unterstützen, die auf anderen Plattformen und anderen Windows-Betriebssystemen basieren.

Das Windows-Betriebssystem implementiert einen Standardsatz von Authentifizierungs Protokollen, einschließlich Kerberos, NTLM, Transport Layer Security/Secure Sockets Layer (TLS/SSL-)und Digest als Teil einer erweiterbaren Architektur. Darüber hinaus werden einige Protokolle zu Authentifizierungspaketen zusammengefasst, beispielsweise Negotiate und der Credential Security Support Provider. Mit diesen Protokollen und Paketen können Benutzer, Computer und Dienste authentifiziert werden. Der Authentifizierungsprozess wiederum ermöglicht Benutzern und Diensten einen sicheren Zugriff auf Ressourcen.

Weitere Informationen zur Windows-Authentifizierung einschließlich der Aspekte

- [Windows-Authentifizierungskonzepte](#)
- [Windows-Anmeldeszenarios](#)
- [Architektur der Windows-Authentifizierung](#)
- [Architektur der Security Support Provider-Schnittstelle](#)

- [Anmeldeinformationen-Prozesse in der Windows-Authentifizierung](#)
- [In der Windows-Authentifizierung verwendete Gruppenrichtlinieneinstellungen](#)

Weitere Informationen finden Sie unter [Technische Übersicht zur Windows-Authentifizierung](#).

Praktische Anwendungsfälle

Mithilfe der Windows-Authentifizierung wird überprüft, ob die Informationen von einer vertrauenswürdigen Quelle stammen, ungeachtet dessen, ob es sich um eine Person oder ein Computerobjekt, beispielsweise einen anderen Computer, handelt. Windows stellt viele verschiedene Methoden bereit, um dies zu erreichen. Im Folgenden werden diese Methoden beschrieben.

| AN... | FEATURE | BESCHREIBUNG |
|--|---|--|
| Authentifizieren innerhalb einer Active Directory-Domäne | Kerberos | <p>Die Microsoft Windows Server-Betriebssysteme implementieren das Kerberos Version 5-Authentifizierungsprotokoll und Erweiterungen für die Authentifizierung mit öffentlichem Schlüssel. Der Kerberos-Authentifizierungs Client wird als Security Support Provider (SSP-) implementiert, und der Zugriff erfolgt über die Security Support Provider-Schnittstelle (SSPI-). Die anfängliche Benutzerauthentifizierung ist in das Winlogon--für einmaliges Anmelden integriert. Die Kerberos-Schlüsselverteilungscenter (KDC-) ist in andere Windows Server-Sicherheitsdienste integriert, die auf dem Domänen Controller ausgeführt werden. Der KDC verwendet die Active Directory Verzeichnisdienst-Datenbank der Domäne als Sicherheits Konto Datenbank. Active Directory ist für Standardimplementierungen von Kerberos erforderlich.</p> <p>Weitere Ressourcen finden Sie unter Kerberos-Authentifizierung: Übersicht.</p> |
| Sichere Authentifizierung im Web | TLS/SSL wie im SChannel Security Support Provider implementiert | <p>Die Transport Layer Security (TLS) Protokoll Versionen 1,0, 1,1 und 1,2, Secure Sockets Layer (SSL) Protokoll, Versionen 2,0 und 3,0, Datagram Transport Layer Security Protokollversion 1,0 und der private Communications Transport (PCT) Protocol, Version 1,0, basieren auf Kryptografie mit öffentlichem Schlüssel. Die Secure Channel (SChannel) Provider Authentication Protocol Suite stellt diese Protokolle bereit. Alle SChannel-Protokolle verwenden ein Client- und Servermodell.</p> <p>Weitere Ressourcen finden Sie unter TLS-SSL (Schannel SSP) Overview.</p> |

| AN... | FEATURE | BESCHREIBUNG |
|---|--|--|
| Authentifizieren bei einem Webdienst oder einer Anwendung | Integrierte Windows-Authentifizierung
Digestauthentifizierung | Weitere Ressourcen finden Sie unter integrierte Windows-Authentifizierung und Digestauthentifizierung und Erweiterte Digestauthentifizierung .
Digest Authentication |
| Authentifizieren bei älteren Anwendungen | NTLM | NTLM ist eine Herausforderung-Authentifizierungsprotokoll für den Antwort Stil. Zusätzlich zur Authentifizierung bietet das NTLM-Protokoll optional eine Sitzungs Sicherheit, insbesondere Nachrichten Integrität und Vertraulichkeit durch Signierungs-und Versiegelung von Funktionen in NTLM.

Weitere Ressourcen finden Sie unter NTLM: Übersicht . |
| Nutzen der mehrstufigen Authentifizierung | Unterstützung von Smartcards
Biometrie-Unterstützung | Smartcards sind eine Manipulations geschützte-, um Sicherheitslösungen für Aufgaben wie Client Authentifizierung, Anmeldung bei Domänen, Code Signatur und Sicherung von e-Mail bereitzustellen.

Bei der Biometrie wird ein unveränderliches physisches Merkmal einer Person erfasst, um diese Person eindeutig identifizieren zu können. Fingerabdrücke gehören zu den am häufigsten genutzten biometrischen Merkmalen, weshalb Millionen PCs und Peripheriegeräte mit biometrischen Fingerabdrucklesern ausgestattet sind.

Weitere Ressourcen finden Sie unter Technische Referenz zu Smartcards . |
| Bereitstellen der lokalen Verwaltung, Speicherung und Wiederverwendung von Anmeldeinformationen | Verwaltung von Anmeldeinformationen
Lokale Sicherheitsautorität

Kennwörter | Durch die Verwaltung von Anmeldeinformationen in Windows wird sichergestellt, Anmeldeinformationen sicher gespeichert werden. Anmelde Informationen werden auf dem sicheren Desktop (für den lokalen oder Domänen Zugriff)über apps oder Websites gesammelt, sodass bei jedem Zugriff auf eine Ressource die richtigen Anmelde Informationen angezeigt werden. |
| Erweitern des Authentifizierungsschutzes auf Legacysysteme | Erweiterter Schutz für Authentifizierung | Diese Funktion verbessert den Schutz und die Handhabung von Anmelde Informationen bei der Authentifizierung von Netzwerkverbindungen mithilfe der integrierten Windows-Authentifizierung (IWA). |

Softwareanforderungen

Die Windows-Authentifizierung ist so konzipiert, dass sie mit früheren Versionen des Windows-Betriebssystems kompatibel ist. Verbesserungen in einer neuen Version stehen jedoch nicht notwendigerweise auch in früheren Versionen zur Verfügung. Weitere Informationen finden Sie in der Dokumentation zu den verschiedenen Features.

Informationen zum Server-Manager

Viele Authentifizierungsfeatures können mit der Gruppenrichtlinie konfiguriert werden, die mithilfe des Server-Managers installiert werden kann. Das Windows-Biometrieframework wird mithilfe des Server-Managers installiert. Andere Serverrollen, die von Authentifizierungsmethoden abhängig sind, z. B. Webserver (IIS) und Active Directory Domain Services, können auch mit Server-Manager installiert werden.

Verwandte Ressourcen

| AUTHENTIFIZIERUNGSTECHNOLOGIEN | RESSOURCEN |
|---|---|
| Windows-Authentifizierung | Windows-Authentifizierung: Technische Übersicht
Enthält Themen, in denen Unterschiede zwischen Versionen, allgemeinen Authentifizierungskonzepten, Anmelde-Szenarien, Architekturen für unterstützte Versionen und anwendbaren Einstellungen behandelt werden. |
| Kerberos | Kerberos-Authentifizierung (Übersicht)
Übersicht zu Kerberos Constrained Delegation

Technische Referenz für die Kerberos-Authentifizierung(2003)

Kerberos-Lebens Handbuch (TechNet-wiki) |
| TLS/SSL und DTLS (SChannel Security Support Provider) | TLS-SSL (Schannel SSP) (Übersicht)
Schannel Security Support Provider: Technische Referenz |
| Digestauthentifizierung | Technische Referenz für die Digest-Authentifizierung(2003) |
| NTLM | Übersicht über NTLM
Enthält Links zu aktuellen und früheren Ressourcen |
| PKU2U | Einführung in PKU2U in Windows |
| Smartcard | Technische Referenz zu Smartcards |
| Anmeldeinformationen | Schutz und Verwaltung von Anmeldeinformationen
Enthält Links zu aktuellen und früheren Ressourcen
Übersicht über Kennwörter
Enthält Links zu aktuellen und früheren Ressourcen |

Windows-Authentifizierung: Technische Übersicht

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Thema für IT-Experten enthält Links zu Themen für die technische Übersicht über die Windows-Authentifizierung. Die Windows-Authentifizierung ist der Prozess, mit dem die Authentizität eines Benutzers oder dienstanzversuchs nachgewiesen werden kann, der auf Windows

In dieser Sammlung von Themen werden die Architektur der Windows-Authentifizierung und deren Komponenten beschrieben.

Klicken Sie zum digitalen Speichern oder Drucken von Seiten aus dieser Bibliothek auf **Exportieren** (oben rechts auf der Seite), und folgen Sie dann den Anweisungen.

- [Unterschiede bei der Windows-Authentifizierung zwischen Windows-Betriebssystemen](#)

Beschreibt die wesentlichen Unterschiede in der Authentifizierungs Architektur und den Prozessen.

- [Windows-Authentifizierungskonzepte](#)

Beschreibt die Konzepte, auf denen die Windows-Authentifizierung basiert.

- [Szenarien für die Windows-Anmelde Authentifizierung](#)

Fasst die verschiedenen Anmelde Szenarien zusammen.

- [Architektur der Windows-Authentifizierung](#)

Beschreibt die wesentlichen Unterschiede in der Authentifizierungs Architektur und den Prozessen für Windows-Betriebssysteme.

- [Architektur der Security Support Provider-Schnittstelle](#)

Beschreibt die SSPI-Architektur.

- [Anmeldeinformationen-Prozesse in der Windows-Authentifizierung](#)

Beschreibt die verschiedenen Prozesse zur Verwaltung von Anmelde Informationen.

- [Bei der Windows-Authentifizierung verwendete Gruppenrichtlinien](#)

Beschreibt die Verwendung und Auswirkung von Gruppenrichtlinien in den Authentifizierungsprozess.

Nicht abgedeckte Elemente

Diese Themensammlung behandelt keine Prozeduren für das Entwerfen, implementieren oder Überwachen von Authentifizierungs Technologien innerhalb einer Windows-Umgebung.

- Entwurfs Informationen zu Windows-Autorisierungs Strategien finden Sie unter [Entwerfen einer Ressourcen Autorisierungs Strategie](#).
- Entwurfs Informationen zu Windows-Authentifizierungs Strategien finden Sie unter [Entwerfen einer Authentifizierungs Strategie](#).
- Entwurfs Informationen zu den Implementierungs Strategien für die Public Key-Infrastruktur von Windows finden Sie unter [Entwerfen einer Public Key-Infrastruktur](#).

- Informationen zum Konfigurieren und Überwachen der Sicherheit, einschließlich der Authentifizierung, in Ihrer Windows-Umgebung finden Sie unter:
 - [Windows XP-Sicherheitshandbuch](#)
 - [Windows Vista-Sicherheitsbaseline](#)
 - [Windows Server 2003-Sicherheitsbaseline](#) und das [Handbuch zu Bedrohungen und Gegenmaßnahmen](#)
 - [Windows Server 2008-Sicherheitshandbuch](#)
 - [Windows Server 2008 R2-Sicherheitsbaseline](#)
- Informationen zum Überwachen von Anmelde- und Authentifizierungs Ereignissen in Windows finden Sie unter Überwachen von [Sicherheits Ereignissen](#).

Windows-Authentifizierungskonzepte

09.04.2020 • 23 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Referenz Übersichts Thema werden die Konzepte beschrieben, auf denen die Windows-Authentifizierung basiert.

Authentifizierung ist der Vorgang, durch den die Identität eines Objekts oder einer Person überprüft wird. Ziel der Authentifizierung eines Objekts ist es, sicherzustellen, dass das Objekt echt und unverfälscht ist. Wenn Sie eine Person authentifizieren, besteht das Ziel darin, zu überprüfen, ob die Person kein Imposter ist.

Im Netzwerkkontext dient die Authentifizierung dazu, die Identität gegenüber einer Netzwerkanwendung oder -ressource nachzuweisen. In der Regel wird die Identität durch einen kryptografischen Vorgang nachgewiesen, der einen Schlüssel verwendet, der nur dem Benutzer bekannt ist (wie bei der Kryptografie mit öffentlichem Schlüssel) oder ein gemeinsam verwendeter Schlüssel. Auf der Serverseite der Authentifizierungskommunikation werden die signierten Daten mit einem bekannten Kryptografieschlüssel verglichen, um den Authentifizierungsversuch zu überprüfen.

Durch die Speicherung der Kryptografieschlüssel an einem zentralen Ort wird der Authentifizierungsvorgang skalierbar und verwaltbar. Active Directory ist die empfohlene und Standardtechnologie zum Speichern von Identitätsinformationen, die die kryptografischen Schlüssel enthalten, bei denen es sich um die Anmeldeinformationen des Benutzers handelt. Active Directory ist für Standardimplementierungen von Kerberos und NTLM erforderlich.

Die Authentifizierungstechniken reichen von der einfachen Anmeldung bei einem Betriebssystem oder der Anmeldung bei einem Dienst oder einer Anwendung, der Benutzer auf der Grundlage von etwas, das nur dem Benutzer bekannt ist (z. b. ein Kennwort), zu leistungsfähigeren Sicherheitsmechanismen, die von Benutzern verwendet werden, wie z. b. Token, öffentliche Schlüssel Zertifikate, Bilder oder biologische Attribute, identifiziert. In einer Unternehmensumgebung ist es Benutzer eventuell möglich, auf unterschiedliche Anwendungen auf verschiedenen Arten von Servern an einem einzigen Standort oder auch standortübergreifend zugreifen. Aus diesem Grund muss die Authentifizierung Umgebungen unterstützen, die auf anderen Plattformen und anderen Windows-Betriebssystemen basieren.

Authentifizierung und Autorisierung: eine Reise Analogie

Eine Reise Analogie kann Ihnen helfen, die Funktionsweise der Authentifizierung zu erläutern. In der Regel sind einige Vorbereitungsaufgaben erforderlich, um die Journey zu beginnen. Der Reisende muss seine tatsächliche Identität seinen Host Behörden nachweisen. Diese Prüfung kann in Form von Nachweis der Bürgerschaft, Geburts Stelle, persönlichen gutschäfts-, Foto-und Foto-oder sonstigen Anforderungen des Gastlandes erfolgen. Die Identität des Reisenden wird durch die Ausstellung eines Passport überprüft. Dies entspricht einem von einer Organisation ausgestellten und verwalteten Systemkonto (dem Sicherheits Prinzipal). Der Passport und das beabsichtigte Ziel basieren auf einer Reihe von Regeln und Vorschriften, die von der behördlichen Behörde ausgestellt wurden.

Die Journey

Wenn der Reisende an der internationalen Grenze eintrifft, fordert ein Border Guard Anmelde Informationen an, und der Reiseleiter zeigt seinen Passport an. Der Prozess ist zweifache:

- Der Schutz authentifiziert den Passport, indem er überprüft, ob er von einer Sicherheits Autorität ausgestellt

wurde, die von der lokalen Regierung als vertrauenswürdig eingestuft wird.

- Der Wächter authentifiziert den Benutzer, indem er überprüft, ob das Gesicht mit dem Gesicht der Person übereinstimmt, die auf dem Passport abgebildet ist, und dass andere erforderliche Anmelde Informationen in Ordnung sind.

Wenn der Passport-Wert gültig ist und der Reisende seinen Besitzer bestätigt, ist die Authentifizierung erfolgreich, und dem Reisenden kann der Zugriff über den Rahmen gestattet werden.

Transitive Vertrauensstellung zwischen Sicherheitsbehörden ist die Grundlage für die Authentifizierung. der Authentifizierungstyp, der an einem internationalen Rahmen stattfindet, basiert auf der Vertrauensstellung. Die lokale Regierung kennt den Reisenden nicht, aber Sie vertraut der Host Regierung. Wenn die Host Behörde den Passport ausgestellt hat, hat Sie den Reisenden nicht kennen gelernt. Er hat der Agentur vertraut, die das Geburts Zertifikat oder eine andere Dokumentation ausgestellt hat. Die Agentur, die das Geburts Zertifikat ausgestellt hat, hat wiederum den Arzt, der das Zertifikat signiert hat, als vertrauenswürdig eingestuft. Der Arzt hat den Geburtstag des Reisenden miterlebt und das Zertifikat mit einem direkten Nachweis der Identität versehen, in diesem Fall mit dem Speicherbedarf der Neugeborenen. Vertrauens Stellungen, die auf diese Weise über den vertrauenswürdigen Vermittler übertragen werden, sind transitiv.

Transitive Vertrauensstellung ist die Grundlage für die Netzwerksicherheit in der Windows-Client-/Serverarchitektur. Eine Vertrauensstellung fließt in eine Gruppe von Domänen, wie z. b. eine Domänen Struktur, und bildet eine Beziehung zwischen einer Domäne und allen Domänen, die dieser Domäne vertrauen. Wenn Domäne a z. b. eine transitiv Vertrauensstellung mit Domäne b aufweist und Domäne b Domäne c vertraut, vertraut Domäne a Domäne c.

Es gibt einen Unterschied zwischen Authentifizierung und Autorisierung. Mit der-Authentifizierung beweist das System, dass Sie Sie sind. Mit der Autorisierung überprüft das System, ob Sie über die Rechte verfügen, was Sie tun möchten. Um die Rahmen Analogie zum nächsten Schritt zu übernehmen, ist die reine Authentifizierung, dass der Reisende der ordnungsgemäße Besitzer eines gültigen Passport ist, nicht zwangsläufig autorisiert, den Reisenden in ein Land einzugeben. Die Einwohner eines bestimmten Landes können in ein anderes Land eintreten, indem Sie einfach nur in Situationen, in denen das Land eingegeben wird, eine unbegrenzte Berechtigung für alle Bürger dieses bestimmten Landes gewähren.

Auf ähnliche Weise können Sie allen Benutzern aus einer bestimmten Domäne Berechtigungen für den Zugriff auf eine Ressource gewähren. Jeder Benutzer, der zu dieser Domäne gehört, hat Zugriff auf die Ressource, ebenso wie Kanada es US-Bürgern ermöglicht, Kanada einzugeben. Allerdings haben US-Bürger, die versuchen, in Brasilien oder Indien zu eintreten, festzustellen, dass Sie diese Länder nicht nur durch die Darstellung eines Passport eingeben können Die Authentifizierung garantiert daher nicht den Zugriff auf Ressourcen oder die Autorisierung für die Verwendung von Ressourcen.

Anmeldeinformationen

Ein Passport-und möglicherweise zugeordnetes Visum sind die akzeptierten Anmelde Informationen für einen Reisenden. Mit diesen Anmelde Informationen kann ein Reisender jedoch nicht auf alle Ressourcen in einem Land zugreifen oder darauf zugreifen. Beispielsweise sind für die Teilnahme an einer Konferenz zusätzliche Anmelde Informationen erforderlich. In Windows können Anmelde Informationen verwaltet werden, damit Kontoinhaber über das Netzwerk auf Ressourcen zugreifen können, ohne dass Sie wiederholt ihre Anmelde Informationen angeben müssen. Diese Art des Zugriffs ermöglicht Benutzern das einmalige Authentifizieren von Benutzern, um auf alle Anwendungen und Datenquellen zuzugreifen, für die Sie autorisiert sind, ohne einen anderen Konto Bezeichner oder ein anderes Kennwort einzugeben. Die Windows-Plattform nutzt die Möglichkeit, eine einzelne Benutzeridentität (durch Active Directory) im Netzwerk zu verwenden, indem Benutzer Anmelde Informationen lokal in der lokalen Sicherheits Autorität (LSA) des Betriebssystems zwischengespeichert werden. Wenn sich ein Benutzer bei der Domäne anmeldet, verwenden Windows-Authentifizierungs Pakete die Anmelde Informationen transparent, um beim Authentifizieren der Anmelde Informationen für Netzwerkressourcen Single Sign-on bereitzustellen. Weitere Informationen zu Anmelde Informationen finden Sie unter Anmelde Informationen für

Eine Form der Multi-Factor Authentication für den Reisenden ist möglicherweise die Anforderung, mehrere Dokumente zu übertragen und zu präsentieren, um Ihre Identität zu authentifizieren, z. b. Pass- und Konferenz Registrierungsinformationen. Windows implementiert dieses Formular oder die Authentifizierung mithilfe von Smartcards, virtuellen Smartcards und biometrischen Technologien.

Sicherheits Prinzipale und Konten

In Windows ist jeder Benutzer, jeder Dienst, jede Gruppe oder jeder Computer, der eine Aktion initiieren kann, ein Sicherheits Prinzipal. Sicherheits Prinzipale verfügen über Konten, die auf einem Computer lokal sein können oder Domänen basiert sind. Beispielsweise können Windows-Client Computer, die einer Domäne angehören, an einer Netzwerk Domäne teilnehmen, indem Sie mit einem Domänen Controller kommunizieren, auch wenn kein Benutzer angemeldet ist. Zum Initiieren der Kommunikation muss der Computer über ein aktives Konto in der Domäne verfügen. Vor der Annahme der Kommunikation vom Computer wird die Identität des Computers von der lokalen Sicherheits Autorität auf dem Domänen Controller authentifiziert. Anschließend wird der Sicherheitskontext des Computers genau wie für einen Human Security Principal definiert. Dieser Sicherheitskontext definiert die Identität und die Funktionen eines Benutzers oder Diensts auf einem bestimmten Computer oder einem Benutzer, einem Dienst, einer Gruppe oder einem Computer in einem Netzwerk. Er definiert z. b. die Ressourcen, z. b. eine Dateifreigabe oder einen Drucker, auf die zugegriffen werden kann, sowie die Aktionen, wie z. b. lesen, schreiben oder ändern, die von einem Benutzer, einem Dienst oder einem Computer auf dieser Ressource ausgeführt werden können. Weitere Informationen finden Sie unter [Sicherheits Prinzipale](#).

Ein Konto ist ein Mittel zum Identifizieren eines Anforderer: der Benutzer oder der Dienst, der den Zugriff oder die Ressourcen anfordert. Der Reisende, der den authentischen Passport innehat, verfügt über ein Konto mit dem hostland. Benutzer, Gruppen von Benutzern, Objekten und Diensten können über einzelne Konten oder Freigabe Konten verfügen. Konten können Mitglied von Gruppen sein, und Ihnen können bestimmte Rechte und Berechtigungen zugewiesen werden. Konten können auf den lokalen Computer, die Arbeitsgruppe, das Netzwerk oder die zugewiesene Mitgliedschaft zu einer Domäne beschränkt werden.

Integrierte Konten und die Sicherheitsgruppen, von denen Sie Mitglieder sind, werden für jede Windows-Version definiert. Mithilfe von Sicherheitsgruppen können Sie den gleichen Sicherheits Berechtigungen für viele Benutzer zuweisen, die erfolgreich authentifiziert wurden, wodurch die Zugriffs Verwaltung vereinfacht wird. Regeln für das Ausstellen von Pässen erfordern möglicherweise, dass der Reisende bestimmten Gruppen zugewiesen wird, z. b. Geschäfts-, Touristen- oder Regierungsbehörden. Durch diesen Vorgang wird sichergestellt, dass für alle Mitglieder einer Gruppe konsistente Sicherheits Berechtigungen erteilt werden. Durch die Verwendung von Sicherheitsgruppen zum Zuweisen von Berechtigungen bedeutet dies, dass die Zugriffs Steuerung von Ressourcen konstant und einfach zu verwalten und zu überwachen ist. Durch Hinzufügen und Entfernen von Benutzern, die bei Bedarf Zugriff von den entsprechenden Sicherheitsgruppen benötigen, können Sie die Häufigkeit von Änderungen an Zugriffs Steuerungs Listen (ACLs) minimieren.

Eigenständige verwaltete Dienst Konten und virtuelle Konten wurden in Windows Server 2008 R2 und Windows 7 eingeführt, um erforderliche Anwendungen wie Microsoft Exchange Server und Internetinformationsdienste (IIS) mit der Isolation ihrer eigenen Domänen Konten bereitzustellen, während ein Administrator den Dienst Prinzipal Namen (Service Principal Name, SPN) und die Anmelde Informationen für diese Konten nicht mehr manuell verwalten muss. Gruppen verwaltete Dienst Konten wurden in Windows Server 2012 eingeführt und bieten die gleiche Funktionalität innerhalb der Domäne, erweitern diese Funktionalität aber auch auf mehrere Server. Beim Herstellen einer Verbindung mit einem Dienst, der in einer Serverfarm gehostet wird (beispielsweise ein Netzwerklastenausgleich), erfordern die Authentifizierungsprotokolle mit gegenseitiger Authentifizierung, dass alle Instanzen der Dienste den gleichen Prinzipal verwenden.

Weitere Informationen zu Konten finden Sie unter:

- [Active Directory Konten](#)

- [Sicherheitsgruppen Active Directory](#)
- [Lokale Konten](#)
- [Microsoft-Konten](#)
- [Dienst Konten](#)
- [Besondere Identitäten](#)

Delegierte Authentifizierung

Um die Reise Analogie zu verwenden, können Länder den gleichen Zugriff für alle Mitglieder einer offiziellen behördlichen Delegation ausgeben, so lange die Delegaten bekannt sind. Diese Delegation ermöglicht einem Mitglied das agieren der Autorität eines anderen Mitglieds. In Windows erfolgt die delegierte Authentifizierung, wenn ein Netzwerkdienst eine Authentifizierungsanforderung von einem Benutzer akzeptiert und die Identität dieses Benutzers annimmt, um eine neue Verbindung mit einem zweiten Netzwerkdienst zu initiieren. Zur Unterstützung der delegierten Authentifizierung müssen Sie Front-End-Server oder Server der ersten Ebene einrichten, wie z. b. Webserver, die für die Verarbeitung von Client Authentifizierungsanforderungen und Back-End- oder n-Tier-Servern (z. b. große Datenbanken) verantwortlich sind, die für das Speichern von Informationen verantwortlich sind Sie können das Recht zum Einrichten der delegierten Authentifizierung für Benutzer in Ihrer Organisation delegieren, um die administrative Belastung Ihrer Administratoren zu verringern.

Wenn Sie einen Dienst oder Computer als vertrauenswürdig für die Delegation einrichten, können Sie diesen Dienst oder Computer für die delegierte Authentifizierung festlegen, ein Ticket für den Benutzer erhalten, der die Anforderung sendet, und dann auf Informationen für diesen Benutzer zugreifen. Dieses Modell schränkt den Datenzugriff auf Back-End-Server nur auf die Benutzer oder Dienste ein, die Anmelde Informationen mit den korrekten Zugriffs Steuerungs Token darstellen. Außerdem ermöglicht es die Zugriffs Überwachung für diese Back-End-Ressourcen. Durch die Anforderung, dass auf alle Daten über Anmelde Informationen zugegriffen werden muss, die zur Verwendung im Auftrag des Clients an den Server delegiert werden, stellen Sie sicher, dass der Server nicht kompromittiert werden kann und dass Sie Zugriff auf vertrauliche Informationen erhalten können, die auf anderen Servern gespeichert sind. Die delegierte Authentifizierung ist nützlich für Anwendungen mit mehreren Ebenen, die für die Verwendung Single Sign-On Funktionen auf mehreren Computern konzipiert sind.

Authentifizierung in Vertrauens Stellungen zwischen Domänen

Die meisten Organisationen, die über mehr als eine Domäne verfügen, müssen den Benutzern den Zugriff auf gemeinsam genutzte Ressourcen in einer anderen Domäne erlauben, ebenso wie der Reisende in verschiedene Regionen im Land einreisen darf. Um diesen Zugriff zu steuern, ist es erforderlich, dass Benutzer in einer Domäne auch authentifiziert und autorisiert werden können, Ressourcen in einer anderen Domäne zu verwenden. Zum Bereitstellen von Authentifizierungs- und Autorisierungs Funktionen zwischen Clients und Servern in verschiedenen Domänen muss eine Vertrauensstellung zwischen den beiden Domänen vorhanden sein. Vertrauens Stellungen sind die zugrunde liegende Technologie, mit der gesicherte Active Directory Kommunikation stattfindet und eine integrale Sicherheitskomponente der Windows Server-Netzwerkarchitektur ist.

Wenn eine Vertrauensstellung zwischen zwei Domänen besteht, Vertrauen die Authentifizierungsmechanismen für jede Domäne den Authentifizierungen aus der anderen Domäne. Vertrauens Stellungen unterstützen den kontrollierten Zugriff auf freigegebene Ressourcen in einer Ressourcen Domäne (die vertrauende Domäne), indem Sie überprüfen, ob eingehende Authentifizierungsanforderungen von einer vertrauenswürdigen Zertifizierungsstelle stammen, der vertrauenswürdigen Domäne. Auf diese Weise fungieren Vertrauens Stellungen als Bridges, bei denen nur überprüfte Authentifizierungsanforderungen zwischen Domänen übertragen werden können.

Wie eine bestimmte Vertrauensstellung Authentifizierungsanforderungen übergibt, hängt von der Konfiguration ab. Vertrauens Stellungen können unidirektional sein, indem der Zugriff von der vertrauenswürdigen Domäne auf Ressourcen in der vertrauenden Domäne bereitgestellt wird (oder bidirektional), indem der Zugriff von jeder

Domäne auf Ressourcen in der anderen Domäne gewährt wird. Vertrauensstellungen sind ebenfalls nicht transitiv. In diesem Fall besteht nur eine Vertrauensstellung zwischen den beiden vertrauenswürdigen Partner Domänen oder transitiv. In diesem Fall wird die Vertrauensstellung automatisch auf alle anderen Domänen ausgedehnt, denen beide Partner vertraut sind.

Informationen zur Funktionsweise einer Vertrauensstellung finden Sie unter [Funktionsweise von Domänen- und Gesamtstruktur-Vertrauensstellungen](#).

Protokoll Übergang

Der Protokoll Übergang unterstützt Anwendungsentwickler, indem es Anwendungen ermöglicht, verschiedene Authentifizierungsmechanismen auf der Benutzer Authentifizierungsebene zu unterstützen und in den nachfolgenden Anwendungsebenen auf das Kerberos-Protokoll für Sicherheitsfeatures wie z. B. gegenseitige Authentifizierung und eingeschränkte Delegation zu wechseln.

Weitere Informationen zum Protokoll Übergang finden Sie unter [Kerberos-Protokoll Übergang und eingeschränkte Delegation](#).

Eingeschränkte Delegation

Die eingeschränkte Delegation bietet Administratoren die Möglichkeit, Anwendungs Vertrauensstellungs Grenzen anzugeben und zu erzwingen, indem Sie den Bereich einschränken, in dem Anwendungsdienste im Auftrag eines Benutzers agieren können. Sie können bestimmte Dienste angeben, von denen ein Computer, der für die Delegation vertrauenswürdig ist, Ressourcen anfordern kann. Die Flexibilität, Autorisierungsrechte für Dienste einzuschränken, trägt dazu bei, den Entwurf der Anwendungssicherheit zu verbessern, indem die Möglichkeiten der Gefährdung durch nicht vertrauenswürdige Dienste verringert werden.

Weitere Informationen zur eingeschränkten Delegation finden Sie unter [Übersicht über die eingeschränkte Kerberos-Delegation](#).

Siehe auch

[Technische Übersicht über die Windows-Anmeldung und-Authentifizierung](#)

Windows-Anmeldeszenarios

09.04.2020 • 13 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Referenz Thema für IT-Experten werden gängige Windows-Anmelde-und-Anmelde Szenarien zusammengefasst.

Die Windows-Betriebssysteme erfordern, dass sich alle Benutzer bei dem Computer mit einem gültigen Konto anmelden, um auf lokale und Netzwerkressourcen zuzugreifen. Auf Windows-basierten Computern werden Ressourcen durch Implementieren des Anmelde Prozesses, in dem die Benutzer authentifiziert werden, geschützt. Nachdem ein Benutzer authentifiziert wurde, implementieren Autorisierungs-und Zugriffs Steuerungstechnologien die zweite Phase des Schutzes von Ressourcen: ermitteln, ob der authentifizierte Benutzer für den Zugriff auf eine Ressource autorisiert ist.

Der Inhalt dieses Themas gilt für Windows-Versionen, die in der Liste **gilt für** am Anfang dieses Themas angegeben sind.

Darüber hinaus können Anwendungen und Dienste erfordern, dass sich Benutzer anmelden, um auf die Ressourcen zuzugreifen, die von der Anwendung oder dem Dienst angeboten werden. Der Anmeldevorgang ähnelt dem Anmeldevorgang, da ein gültiges Konto und korrekte Anmelde Informationen erforderlich sind. Anmelde Informationen werden jedoch in der SAM-Datenbank (Security Account Manager) auf dem lokalen Computer und ggf. in Active Directory gespeichert. Anmelde Konto-und Anmelde Informationen werden von der Anwendung oder dem Dienst verwaltet und können optional lokal im Schließfach für Anmelde Informationen gespeichert werden.

Informationen zur Funktionsweise der Authentifizierung finden Sie unter [Konzepte der Windows-Authentifizierung](#).

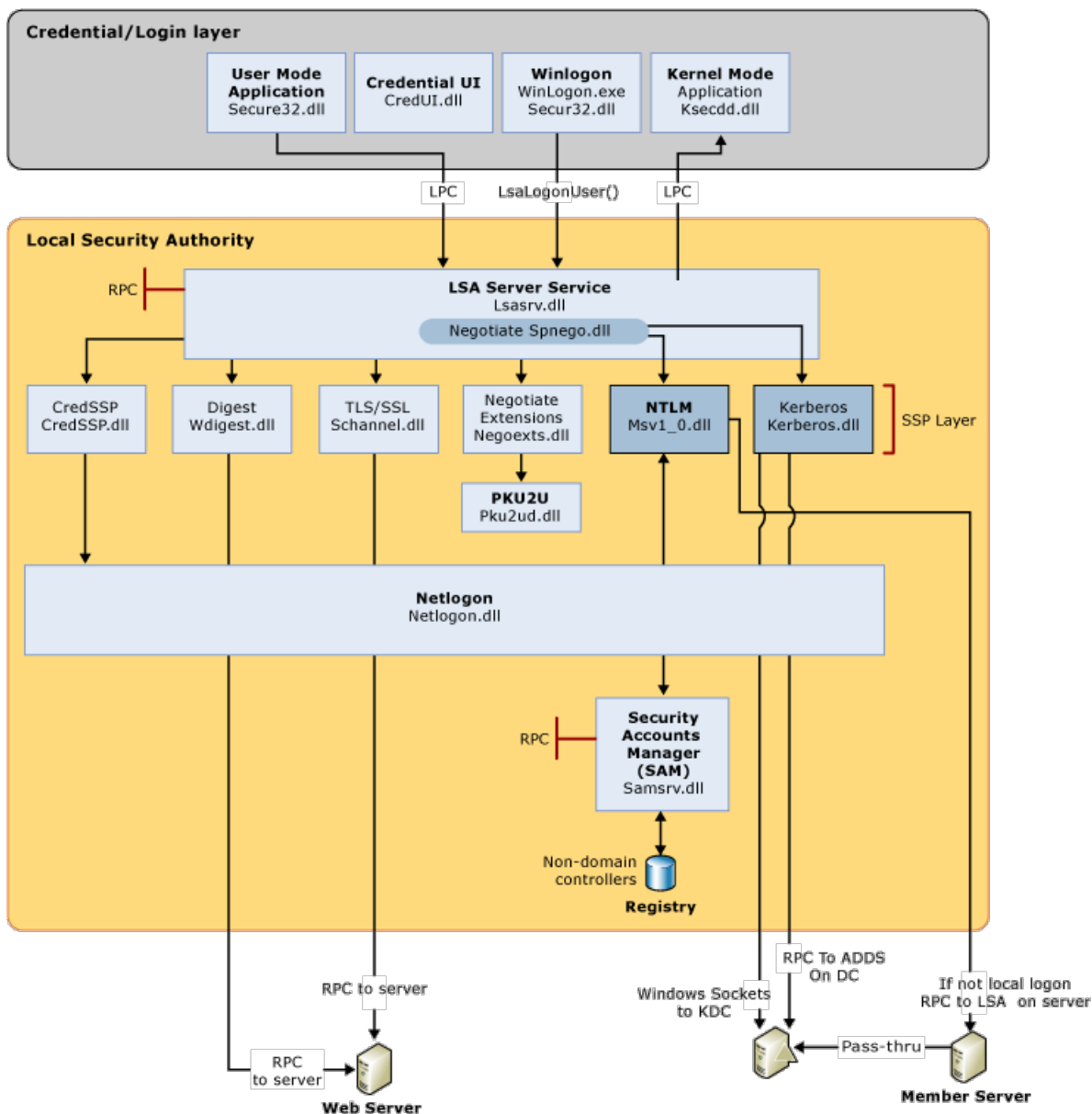
In diesem Thema werden folgende Szenarien beschrieben:

- [Interaktive Anmeldung](#)
- [Netzwerk Anmeldung](#)
- [Smartcardanmeldung](#)
- [Biometrische Anmeldung](#)

Interaktive Anmeldung

Der Anmeldevorgang beginnt entweder dann, wenn ein Benutzer Anmelde Informationen im Dialogfeld Anmelde Informationen eingibt, oder wenn der Benutzer eine Smartcard in den Smartcardleser einfügt oder wenn der Benutzer mit einem biometrischen Gerät interagiert. Benutzer können eine interaktive Anmeldung durchführen, indem Sie ein lokales Benutzerkonto oder ein Domänen Konto verwenden, um sich an einem Computer anzumelden.

Das folgende Diagramm zeigt die interaktiven Anmelde Elemente und den Anmeldevorgang.



Architektur der Windows-Client Authentifizierung

Lokale und Domänen Anmeldung

Die Anmelde Informationen, die der Benutzer für eine Domänen Anmeldung anzeigt, enthalten alle Elemente, die für eine lokale Anmeldung erforderlich sind, z. B. Konto Name, Kennwort oder Zertifikat und Active Directory Domänen Informationen. Der Prozess bestätigt die Identifizierung des Benutzers für die Sicherheitsdatenbank auf dem lokalen Computer des Benutzers oder einer Active Directory Domäne. Dieser obligatorische Anmeldevorgang kann nicht für Benutzer in einer Domäne ausgeschaltet werden.

Benutzer können auf zwei Arten eine interaktive Anmeldung an einem Computer ausführen:

- Lokal, wenn der Benutzer direkten physischen Zugriff auf den Computer hat oder wenn der Computer zu einem Netzwerk von Computern gehört.

Eine lokale Anmeldung gewährt einem Benutzer die Berechtigung für den Zugriff auf Windows-Ressourcen auf dem lokalen Computer. Eine lokale Anmeldung erfordert, dass der Benutzer über ein Benutzerkonto in der Sicherheits Konten Verwaltung (Security Accounts Manager, Sam) auf dem lokalen Computer verfügt. Sam schützt und verwaltet Benutzer-und Gruppeninformationen in Form von Sicherheits Konten, die in der lokalen Computer Registrierung gespeichert sind. Der Computer kann über Netzwerk Zugriff verfügen, ist jedoch nicht erforderlich. Informationen zu lokalen Benutzerkonten und Gruppenmitgliedschaften werden verwendet, um den Zugriff auf lokale Ressourcen zu verwalten.

Bei einer Netzwerk Anmeldung wird dem Benutzer die Berechtigung zum Zugriff auf Windows-Ressourcen

auf dem lokalen Computer zusätzlich zu allen Ressourcen auf vernetzten Computern erteilt, die durch das Zugriffs Token der Anmelde Informationen definiert werden. Sowohl bei einer lokalen Anmeldung als auch bei einer Netzwerk Anmeldung ist es erforderlich, dass der Benutzer über ein Benutzerkonto im Sicherheits Konten Manager (Security Accounts Manager, Sam) auf dem lokalen Computer verfügt. Informationen zu lokalen Benutzerkonten und Gruppenmitgliedschaften werden verwendet, um den Zugriff auf lokale Ressourcen zu verwalten, und das Zugriffs Token für den Benutzer definiert, auf welche Ressourcen auf vernetzten Computern zugegriffen werden kann.

Eine lokale Anmeldung und eine Netzwerk Anmeldung sind nicht ausreichend, um dem Benutzer und dem Computer die Berechtigung zum Zugriff auf und zur Verwendung von Domänen Ressourcen zu erteilen.

- Remote, über Terminal Dienste oder Remotedesktopdienste (RDS). in diesem Fall wird die Anmeldung als Remote interaktiv qualifiziert.

Nach einer interaktiven Anmeldung führt Windows Anwendungen im Namen des Benutzers aus, und der Benutzer kann mit diesen Anwendungen interagieren.

Eine lokale Anmeldung gewährt einem Benutzer die Berechtigung für den Zugriff auf Ressourcen auf dem lokalen Computer oder auf Ressourcen auf vernetzten Computern. Wenn der Computer einer Domäne hinzugefügt wird, versucht die Winlogon-Funktion, sich bei dieser Domäne anzumelden.

Eine Domänen Anmeldung gewährt einem Benutzer die Berechtigung, auf lokale und Domänen Ressourcen zuzugreifen. Eine Domänen Anmeldung erfordert, dass der Benutzer über ein Benutzerkonto in Active Directory verfügt. Der Computer muss über ein Konto in der Active Directory Domäne verfügen und physisch mit dem Netzwerk verbunden sein. Benutzer müssen auch über die Benutzerrechte verfügen, um sich an einem lokalen Computer oder einer Domäne anzumelden. Informationen zu Domänen Benutzerkonten und Gruppenmitgliedschaften werden verwendet, um den Zugriff auf Domänen-und lokale Ressourcen zu verwalten.

Remote Anmeldung

In Windows basiert der Zugriff auf einen anderen Computer über die Remote Anmeldung auf der Remotedesktopprotokoll (RDP). Da sich der Benutzer vor dem Versuch, eine Remote Verbindung herzustellen, bereits erfolgreich am Client Computer angemeldet haben muss, wurden interaktive Anmeldevorgänge erfolgreich abgeschlossen.

RDP verwaltet die Anmelde Informationen, die der Benutzer mit dem Remotedesktop-Client eingibt. Diese Anmelde Informationen sind für den Zielcomputer gedacht, und der Benutzer muss über ein Konto auf diesem Bereitstellungs Zielcomputer verfügen. Außerdem muss der Bereitstellungs Zielcomputer so konfiguriert sein, dass eine Remote Verbindung akzeptiert wird. Zum Versuch, den Authentifizierungsprozess auszuführen, werden die Anmelde Informationen des Ziel Computers gesendet. Wenn die Authentifizierung erfolgreich ist, wird der Benutzer mit lokalen Ressourcen und Netzwerkressourcen verbunden, auf die über die angegebenen Anmelde Informationen zugegriffen werden kann.

Netzwerk Anmeldung

Eine Netzwerk Anmeldung kann nur verwendet werden, nachdem eine Benutzer-, Dienst-oder Computer Authentifizierung stattfindet. Während der Netzwerk Anmeldung verwendet der Prozess nicht die Anmelde Informationen für die Anmelde Informationen, um Daten zu sammeln. Stattdessen werden zuvor festgelegte Anmelde Informationen oder eine andere Methode zum Sammeln von Anmelde Informationen verwendet. Bei diesem Vorgang wird die Identität des Benutzers an jeden Netzwerkdienst bestätigt, auf den der Benutzer zugreifen möchte. Dieser Prozess ist in der Regel für den Benutzer unsichtbar, es sei denn, es müssen alternative Anmelde Informationen angegeben werden.

Um diese Art der Authentifizierung bereitzustellen, umfasst das Sicherheitssystem die folgenden Authentifizierungsmechanismen:

- Kerberos 5-Protokoll

- Zertifikate für öffentliche Schlüssel
- Secure Sockets Layer/Transport Layer Security (SSL/TLS)
- Digest
- NTLM für Kompatibilität mit Microsoft Windows NT 4,0-basierten Systemen

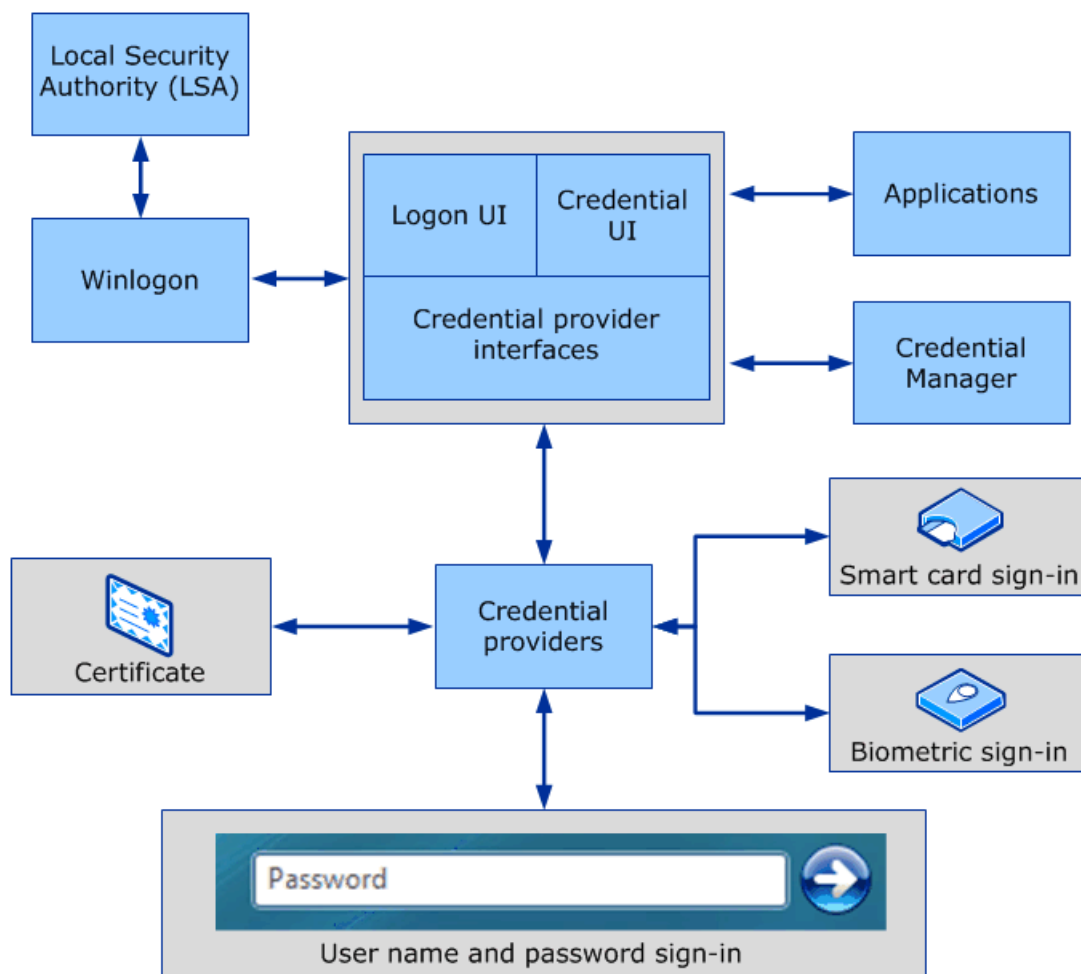
Informationen zu den Elementen und Prozessen finden Sie im obigen interaktiven Anmelde Diagramm.

Smartcardanmeldung

Smartcards können verwendet werden, um sich ausschließlich bei Domänen Konten anzumelden, nicht bei lokalen Konten. Die Smartcard-Authentifizierung erfordert die Verwendung des Kerberos-Authentifizierungs Protokolls. In Windows 2000 Server eingeführt wurde, wird in Windows-basierten Betriebssystemen eine Erweiterung des öffentlichen Schlüssels für die anfängliche Authentifizierungsanforderung des Kerberos-Protokolls implementiert. Im Gegensatz zur Kryptografie mit dem gemeinsamen geheimen Schlüssel ist die Kryptografie mit öffentlichem Schlüssel asymmetrisch, d. h., es sind zwei verschiedene Schlüssel erforderlich: eine zum Verschlüsseln, eine andere zum Entschlüsseln. Die Schlüssel, die zum Ausführen beider Vorgänge erforderlich sind, bilden gemeinsame private/öffentliche Schlüsselpaare.

Um eine typische Anmelde Sitzung zu initiieren, muss ein Benutzer seine Identität nachweisen, indem er Informationen bereitstellt, die nur dem Benutzer und der zugrunde liegenden Kerberos-Protokoll Infrastruktur bekannt sind. Die geheimen Informationen sind ein kryptografischer, gemeinsam verwendeter Schlüssel, der aus dem Kennwort des Benutzers abgeleitet wurde. Ein gemeinsamer geheimer Schlüssel ist symmetrisch. Dies bedeutet, dass derselbe Schlüssel sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet wird.

Das folgende Diagramm zeigt die für die Smartcardanmeldung erforderlichen Elemente und Prozesse.



Smartcard-Anmelde Informationsanbieter-Architektur

Wenn eine Smartcard anstelle eines Kennworts verwendet wird, wird ein privates/öffentliches Schlüsselpaar, das auf der Smartcard des Benutzers gespeichert ist, durch den gemeinsamen geheimen Schlüssel ersetzt, der aus dem Kennwort des Benutzers abgeleitet ist. Der private Schlüssel wird nur auf der Smartcard gespeichert. Der öffentliche Schlüssel kann allen Benutzern zur Verfügung gestellt werden, für die der Besitzer vertrauliche Informationen austauschen möchte.

Weitere Informationen zum Anmeldevorgang für Smartcards in Windows finden Sie unter [Funktionsweise der Smartcard-Anmeldung in Windows](#).

Biometrische Anmeldung

Ein Gerät wird zum Erfassen und Erstellen eines digitalen Merkmals eines Artefakts verwendet, z. b. eines Fingerabdrucks. Diese digitale Darstellung wird dann mit einem Beispiel desselben Artefakts verglichen, und wenn die beiden erfolgreich verglichen werden, kann die Authentifizierung erfolgen. Computer mit einem der in der Liste **gilt für** am Anfang dieses Themas angegebenen Betriebssysteme können so konfiguriert werden, dass Sie diese Art der Anmeldung akzeptieren. Wenn die biometrische Anmeldung jedoch nur für die lokale Anmeldung konfiguriert ist, muss der Benutzer beim Zugriff auf eine Active Directory Domäne Domänen Anmelde Informationen darstellen.

Weitere Ressourcen

Informationen zur Verwaltung von Anmelde Informationen, die während der Anmeldung übermittelt werden, finden Sie unter [Verwaltung von Anmelde Informationen in der Windows-Authentifizierung](#).

[Technische Übersicht über die Windows-Anmeldung und-Authentifizierung](#)

Architektur der Windows-Authentifizierung

09.04.2020 • 4 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Übersichts Thema für IT-Experten erläutert das grundlegende architektonische Schema für die Windows-Authentifizierung.

Die Authentifizierung ist der Prozess, bei dem das System die Anmelde-oder Anmelde Informationen eines Benutzers überprüft. Der Name und das Kennwort eines Benutzers werden mit einer autorisierten Liste verglichen, und wenn das System eine Entsprechung erkennt, wird der Zugriff auf den in der Berechtigungs Liste für diesen Benutzer angegebenen Wert gewährt.

Im Rahmen einer erweiterbaren Architektur implementieren die Windows Server-Betriebssysteme einen Standardsatz von Authentifizierungs-Sicherheits Support Anbietern, darunter aushandeln, Kerberos-Protokoll, NTLM, Schannel (sicherer Kanal) und Digest. Die Protokolle, die von diesen Anbietern verwendet werden, ermöglichen die Authentifizierung von Benutzern, Computern und Diensten, und der Authentifizierungsprozess ermöglicht autorisierten Benutzern und Diensten, auf sichere Weise auf Ressourcen zuzugreifen.

In Windows Server authentifizieren Anwendungen Benutzer mithilfe der SSPI, um Aufrufe für die Authentifizierung zu abstrahieren. Daher müssen Entwickler die Komplexität spezifischer Authentifizierungsprotokolle nicht verstehen oder Authentifizierungsprotokolle in Ihren Anwendungen erstellen.

Windows Server-Betriebssysteme beinhalten eine Reihe von Sicherheitskomponenten, die das Windows-Sicherheitsmodell bilden. Diese Komponenten stellen sicher, dass Anwendungen keinen Zugriff auf Ressourcen ohne Authentifizierung und Autorisierung erhalten. In den folgenden Abschnitten werden die Elemente der Authentifizierungs Architektur beschrieben.

Lokale Sicherheitsautorität

Bei der lokalen Sicherheits Autorität (Local Security Authority, LSA) handelt es sich um ein geschütztes Subsystem, das Benutzer authentifiziert und auf dem lokalen Computer anmeldet. Außerdem verwaltet LSA Informationen über alle Aspekte der lokalen Sicherheit auf einem Computer (diese Aspekte werden zusammen als lokale Sicherheitsrichtlinie bezeichnet). Außerdem werden verschiedene Dienste für die Übersetzung zwischen Namen und Sicherheits-IDs (SIDs) bereitstellt.

Das Sicherheits Subsystem verfolgt die Sicherheitsrichtlinien und die Konten, die sich auf einem Computersystem befinden, nach. Bei einem Domänen Controller sind diese Richtlinien und Konten diejenigen, die für die Domäne, in der sich der Domänen Controller befindet, wirksam sind. Diese Richtlinien und Konten werden in Active Directory gespeichert. Das LSA-Subsystem bietet Dienste zum Validieren des Zugriffs auf Objekte, zum Überprüfen von Benutzerrechten und zum Erstellen von Überwachungs Meldungen.

Security Support Provider-Schnittstelle

Die Security Support Provider-Schnittstelle (Security Support Provider Interface, SSPI) ist die API, die integrierte Sicherheitsdienste für Authentifizierung, Nachrichten Integrität, Datenschutz von Nachrichten und Sicherheits Qualität für ein beliebiges verteiltes Anwendungsprotokoll erhält.

SSPI ist die Implementierung der Generic Security Service API (GSSAPI). SSPI bietet einen Mechanismus, mit dem eine verteilte Anwendung einen von mehreren Sicherheitsanbietern zum Abrufen einer authentifizierten Verbindung abrufen kann, ohne die Details des Sicherheitsprotokolls kennen zu müssen.

Siehe auch

- [Architektur der Security Support Provider-Schnittstelle](#)
- [Anmeldeinformationen-Prozesse in der Windows-Authentifizierung](#)
- [Windows-Authentifizierung: Technische Übersicht](#)

Architektur der SecuritySupportProvider-Schnittstelle

09.04.2020 • 22 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Referenz Thema für IT-Experten werden die Windows-Authentifizierungsprotokolle beschrieben, die in der SSPI-Architektur (Security Support Provider Interface) verwendet werden.

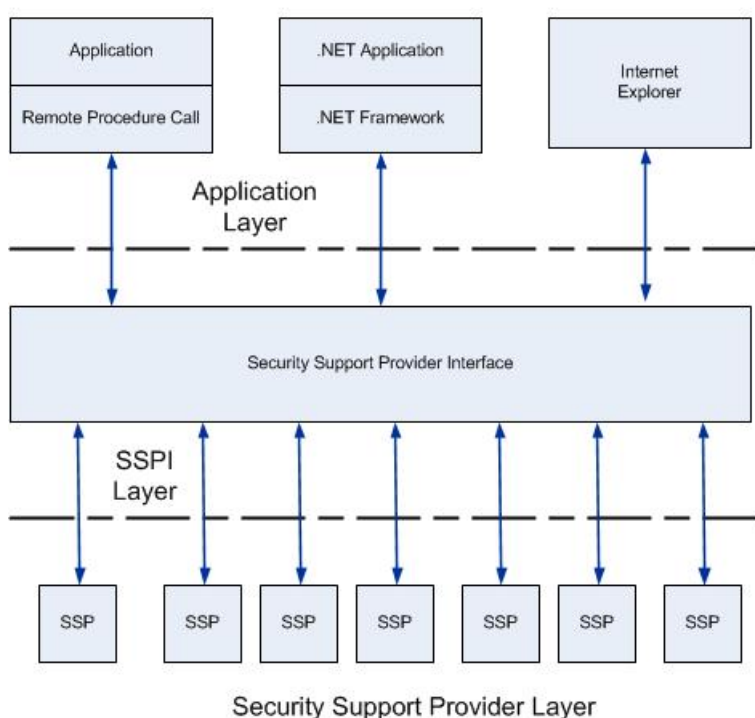
Die Microsoft Security Support Provider-Schnittstelle (SSPI) ist die Grundlage für die Windows-Authentifizierung. Anwendungen und Infrastrukturdienste, die eine Authentifizierung erfordern, verwenden SSPI, um es bereitzustellen.

SSPI ist die Implementierung der generischen Security Service-API (GSSAPI) in Windows Server-Betriebssystemen. Weitere Informationen zu GSSAPI finden Sie unter RFC 2743 und RFC 2744 in der IETF RFC-Datenbank.

Die Standard-SSPs (Security Support Providers), die in Windows bestimmte Authentifizierungsprotokolle aufrufen, sind in die SSPI als DLLs integriert. Diese standardmäßigen SSPs werden in den folgenden Abschnitten beschrieben. Weitere SSPs können integriert werden, wenn Sie mit der SSPI betrieben werden können.

Wie in der folgenden Abbildung gezeigt, stellt die SSPI in Windows einen Mechanismus bereit, der Authentifizierungs Token über den vorhandenen Kommunikationskanal zwischen dem Client Computer und dem Server enthält. Wenn zwei Computer oder Geräte authentifiziert werden müssen, damit Sie sicher kommunizieren können, werden die Authentifizierungsanforderungen an die SSPI weitergeleitet, die den Authentifizierungsvorgang unabhängig vom derzeit verwendeten Netzwerkprotokoll abschließt. Die SSPI gibt transparente binäre große Objekte zurück. Diese werden zwischen den Anwendungen übermittelt. an diesem Punkt können Sie an die SSPI-Schicht übermittelt werden. Auf diese Weise kann eine Anwendung mithilfe der SSPI verschiedene Sicherheitsmodelle verwenden, die auf einem Computer oder Netzwerk verfügbar sind, ohne dass die Schnittstelle zum Sicherheitssystem geändert werden muss.

Security Support Provider Interface Architecture



In den folgenden Abschnitten werden die standardmäßigen SSPs beschrieben, die mit der SSPI interagieren. Die SSPs werden in Windows-Betriebssystemen auf unterschiedliche Weise verwendet, um eine sichere Kommunikation in einer unsicheren Netzwerkumgebung zu fördern.

- [Kerberos-Sicherheits Unterstützungs Anbieter](#)
- [NTLM-Sicherheits Unterstützungs Anbieter](#)
- [Digest-Sicherheits Unterstützungs Anbieter](#)
- [SChannel Security Support Provider](#)
- [Sicherheits Unterstützungs Anbieter aushandeln](#)
- [Anmelde Informationsanbieter für Sicherheitsunterstützung](#)
- [Extensions für den Sicherheitsunterstützungs Anbieter aushandeln](#)
- [PKU2U Security Support Provider](#)

Auch in diesem Thema enthalten:

[Auswahl des Sicherheits Unterstützungs Anbieters](#)

Kerberos-Sicherheits Unterstützungs Anbieter

Dieser SSP verwendet nur das Kerberos 5-Protokoll, das von Microsoft implementiert wird. Dieses Protokoll basiert auf den RFC 4120 und den Entwurfs Revisionen der Netzwerk Arbeitsgruppe. Dabei handelt es sich um ein Industriestandard Protokoll, das mit einem Kennwort oder einer Smartcard für eine interaktive Anmeldung verwendet wird. Es ist auch die bevorzugte Authentifizierungsmethode für Dienste in Windows.

Da das Kerberos-Protokoll seit Windows 2000 das Standard Authentifizierungsprotokoll ist, unterstützen alle Domänen Dienste den Kerberos-SSP. Hierzu gehören:

- Active Directory Abfragen, die das Lightweight Directory Access Protocol (LDAP) verwenden
- Remote Server-oder Arbeitsstations Verwaltung, die den Remote Prozedur aufrufdienst verwendet
- Druckdienste
- Client-Server-Authentifizierung
- Remote Dateizugriff, bei dem das SMB-Protokoll (Server Message Block) verwendet wird (auch bekannt als Common Internet File System oder CIFS)
- Verteilte Dateisystem Verwaltung und-Referenz
- Intranetauthentifizierung zu Internetinformationsdienste (IIS)
- Sicherheits Autoritäts Authentifizierung für die Internet Protokoll Sicherheit (IPSec)
- Zertifikat Anforderungen an Active Directory Zertifikat Dienste für Domänen Benutzer und-Computer

Speicherort:%windir%\windows\system32\kerberos.dll

Dieser Anbieter ist standardmäßig in Versionen enthalten, die in der Liste **gilt für** am Anfang dieses Themas angegeben sind, sowie unter Windows Server 2003 und Windows XP.

Zusätzliche Ressourcen für das Kerberos-Protokoll und den Kerberos-SSP

- [Microsoft Kerberos \(Windows\)](#)
- [\[MS-kile\]: Kerberos-Protokoll Erweiterungen](#)

- [\[MS-SFU\]: Kerberos-Protokoll Erweiterungen: Dienst für Benutzer und eingeschränkte Delegierungs Protokollspezifikation](#)
- [Kerberos SSP/AP \(Windows\)](#)
- [Kerberos-Erweiterungen](#) für Windows Vista
- [Änderungen bei der Kerberos-Authentifizierung](#) für Windows 7
- [Technische Referenz für die Kerberos-Authentifizierung](#)

NTLM-Sicherheits Unterstützungs Anbieter

Der NTLM-Sicherheits Unterstützungs Anbieter (NTLM SSP) ist ein binäres Messaging Protokoll, das von der Security Support Provider-Schnittstelle (SSPI) verwendet wird, um die NTLM-Challenge-Response-Authentifizierung zuzulassen und Integritäts- und Vertraulichkeits Optionen auszuhandeln. NTLM wird verwendet, wenn die SSPI-Authentifizierung verwendet wird, z. b. für Server Message Block oder CIFS-Authentifizierung, http-Aushandlungs Authentifizierung (z. b. Internet-Webauthentifizierung) und den Remote Prozedur aufrufsdienst. Der NTLM-SSP umfasst die NTLM- und NTLM Version 2 (NTLMv2)-Authentifizierungsprotokolle.

Die unterstützten Windows-Betriebssysteme können den NTLM-SSP für Folgendes verwenden:

- Client/Server-Authentifizierung
- Druckdienste
- Dateizugriff mithilfe von CIFS (SMB)
- Sicherer Remote Prozedur aufrufsdienst oder DCOM-Dienst

Speicherort: %windir%\WINDOWS\system32\Msv1_0.dll

Dieser Anbieter ist standardmäßig in Versionen enthalten, die in der Liste **gilt für** am Anfang dieses Themas angegeben sind, sowie unter Windows Server 2003 und Windows XP.

Zusätzliche Ressourcen für das NTLM-Protokoll und den NTLM-SSP

- [MSV1_0 Authentifizierungs Paket \(Windows\)](#)
- [Änderungen bei der NTLM-Authentifizierung](#) in Windows 7
- [Microsoft NTLM \(Windows\)](#)
- [Leitfaden zur Überwachung und Einschränkung der NTLM-Verwendung](#)

Digest-Sicherheits Unterstützungs Anbieter

Die Digest-Authentifizierung ist ein Industriestandard, der für LDAP (Lightweight Directory Access Protocol) und die Webauthentifizierung verwendet wird. Die Digest-Authentifizierung überträgt Anmelde Informationen über das Netzwerk als MD5-Hash oder Nachrichten Digest.

Digest SSP (wdigest.dll) wird für Folgendes verwendet:

- Internet Explorer- und Internetinformationsdienste Zugriff (IIS)
- LDAP-Abfragen

Speicherort: %windir%\windows\system32\digest.dll

Dieser Anbieter ist standardmäßig in Versionen enthalten, die in der Liste **gilt für** am Anfang dieses Themas angegeben sind, sowie unter Windows Server 2003 und Windows XP.

Zusätzliche Ressourcen für das Digest-Protokoll und den Digest-SSP

- [Microsoft Digest Authentifizierung \(Windows\)](#)
- [\[MS-dsp\]: Digest-Protokoll Erweiterungen](#)

SChannel Security Support Provider

Der sichere Kanal (SChannel) wird für die webbasierte Server Authentifizierung verwendet, z. b. Wenn ein Benutzer versucht, auf einen sicheren Webserver zuzugreifen.

Das TLS-Protokoll, das SSL-Protokoll, das PCT-Protokoll (private Communications Technology) und das DTLS-Protokoll (Datagram Transport Layer) basieren auf Kryptografie mit öffentlichem Schlüssel. SChannel stellt alle diese Protokolle bereit. Alle SChannel-Protokolle verwenden ein Client/Server-Modell. Der SChannel SSP verwendet Zertifikate für öffentliche Schlüssel zum Authentifizieren von Parteien. Beim Authentifizieren von Parteien wählt SChannel SSP ein Protokoll in der folgenden Reihenfolge aus:

- Transport Layer Security (TLS) Version 1,0
- Transport Layer Security (TLS) Version 1,1
- Transport Layer Security (TLS) Version 1,2
- Secure Socket Layer (SSL) Version 2,0
- Secure Socket Layer (SSL) Version 3,0
- Private Kommunikationstechnologie (PCT)

Hinweis PCT ist standardmäßig deaktiviert.

Das ausgewählte Protokoll ist das bevorzugte Authentifizierungsprotokoll, das vom Client und vom Server unterstützt werden kann. Wenn ein Server beispielsweise alle SChannel-Protokolle unterstützt und der Client nur SSL 3,0 und SSL 2,0 unterstützt, verwendet der Authentifizierungsprozess SSL 3,0.

DTLS wird verwendet, wenn Sie von der Anwendung explizit aufgerufen wird. Weitere Informationen zu DTLS und den anderen Protokollen, die vom SChannel-Anbieter verwendet werden, finden Sie [unter SChannel Security Support Provider Technical Reference](#).

Speicherort:%windir%\windows\system32\schannel.dll

Dieser Anbieter ist standardmäßig in Versionen enthalten, die in der Liste **gilt für** am Anfang dieses Themas angegeben sind, sowie unter Windows Server 2003 und Windows XP.

NOTE

TLS 1,2 wurde in diesem Anbieter in Windows Server 2008 R2 und Windows 7 eingeführt. DTLS wurde in diesem Anbieter in Windows Server 2012 und Windows 8 eingeführt.

Zusätzliche Ressourcen für die TLS-und SSL-Protokolle und den SChannel SSP

- [Sicherer Kanal \(Windows\)](#)
- [Technische Referenz zu TLS/SSL](#)
- [\[MS-TLSP\]: Transport Layer Security \(TLS\)-Profil](#)

Sicherheits Unterstützungs Anbieter aushandeln

Der einfache und geschützte GSS-API-Aushandlungs Mechanismus (spnetgo) bildet die Grundlage für den Aushandlungs-SSP, der zum Aushandeln eines bestimmten Authentifizierungs Protokolls verwendet werden kann. Wenn eine Anwendung SSPI aufruft, um sich bei einem Netzwerk anzumelden, kann ein SSP zum Verarbeiten der Anforderung angegeben werden. Wenn die Anwendung den Aushandlungs-SSP angibt, analysiert Sie die

Anforderung und wählt den entsprechenden Anbieter für die Verarbeitung der Anforderung auf der Grundlage der vom Kunden konfigurierten Sicherheitsrichtlinien aus.

Spnetgo ist in RFC 2478 angegeben.

In unterstützten Versionen der Windows-Betriebssysteme wählt der Aushandlungs Security Support Provider zwischen dem Kerberos-Protokoll und NTLM aus. Aushandeln wählt das Kerberos-Protokollstandard mäßig aus, es sei denn, das Protokoll kann von einem der an der Authentifizierung beteiligten Systeme verwendet werden, oder die aufrufende Anwendung hat keine ausreichenden Informationen für die Verwendung des Kerberos-Protokolls bereitgestellt.

Speicherort:%windir%\windows\system32\lsasrv.dll

Dieser Anbieter ist standardmäßig in Versionen enthalten, die in der Liste **gilt für** am Anfang dieses Themas angegeben sind, sowie unter Windows Server 2003 und Windows XP.

Weitere Ressourcen für den Aushandlungs-SSP

- [Microsoft aushandeln \(Windows\)](#)
- [\[MS-SPNG\]: Simple und Protected GSS-API-Aushandlungs Mechanismus-Erweiterungen \(spnetgo\)](#)
- [\[MS-N2HT\]: Aushandlungs-und Nego2 http-Authentifizierungsprotokoll Spezifikation](#)

Anmelde Informationsanbieter für Sicherheitsunterstützung

Der Anmelde Informations Sicherheits-Dienstanbieter (Credential Security Service Provider, shdssp) stellt beim Starten neuer terminaldienstendienste und Remotedesktopdienste Sitzungen eine Single Sign-on Benutzer Darstellung (SSO) bereit. Mit "andssp" können Anwendungen die Anmelde Informationen des Benutzers vom Client Computer (mithilfe des Client seitigen SSP) an den Zielservers (über den serverseitigen SSP) delegieren, basierend auf den Richtlinien des Clients. Die Richtlinien für die aufwärtssp werden mithilfe von Gruppenrichtlinie konfiguriert. die Delegierung von Anmelde Informationen ist standardmäßig deaktiviert.

Speicherort:%windir%\windows\system32\kredssp.dll

Dieser Anbieter ist standardmäßig in Versionen enthalten, die in der Liste **gilt für** am Anfang dieses Themas angegeben sind.

Weitere Ressourcen für die Anmelde Informationen SSP

- [\[MS-CSSp\]: die Anmelde Informationsanbieter-Protokollspezifikation \(Security Support Provider, fidssp\)](#)
- [Anmelde Informationen Sicherheits Dienstanbieter und SSO für Terminaldiensteanmeldung](#)

Extensions für den Sicherheitsunterstützungs Anbieter aushandeln

Aushandlungs Erweiterungen (NegoExts) ist ein Authentifizierungs Paket, das die Verwendung von SSPs, außer NTLM oder das Kerberos-Protokoll, für Anwendungen und Szenarios, die von Microsoft und anderen Softwareunternehmen implementiert werden, aushandelt.

Diese Erweiterung des Aushandlungs Pakets ermöglicht die folgenden Szenarien:

- **Umfassende Client Verfügbarkeit innerhalb eines Verbundsystems.** Auf Dokumente kann auf SharePoint-Websites zugegriffen werden, und Sie können mithilfe einer Microsoft Office Anwendung mit vollem Funktionsumfang bearbeitet werden.
- **Umfassende Client Unterstützung für Microsoft Office Services.** Benutzer können sich bei Microsoft Office Services anmelden und eine Microsoft Office Anwendung mit vollem Funktionsumfang verwenden.
- **Gehosteter Microsoft Exchange-Server und Outlook.** Es wurde keine Domänen Vertrauensstellung eingerichtet, da Exchange Server im Web gehostet wird. Outlook verwendet den Windows Live-Dienst, um Benutzer zu authentifizieren.

- **Umfassende Client Verfügbarkeit zwischen Client Computern und Servern.** Die Netzwerk- und Authentifizierungs Komponenten des Betriebssystems werden verwendet.

Das Windows-Aushandlungs Paket behandelt den "NegoExts SSP" auf die gleiche Weise wie für Kerberos und NTLM. "NegoExts.dll" wird beim Start in die lokale System Zertifizierungsstelle (Local System Authority, LSA) geladen. Wenn eine Authentifizierungsanforderung empfangen wird, die auf der Anforderungs Quelle basiert, verhandelt NegoExts zwischen den unterstützten SSPs. Sie sammelt die Anmelde Informationen und Richtlinien, verschlüsselt Sie und sendet diese Informationen an den entsprechenden SSP, in dem das Sicherheits Token erstellt wird.

Die von "NegoExts" unterstützten SSPs sind keine eigenständigen SSPs, wie z. b. Kerberos und NTLM. Wenn die Authentifizierungsmethode aus irgendeinem Grund fehlschlägt, wird im SSP von Negoexs daher eine Authentifizierungsfehler Meldung angezeigt oder protokolliert. Es sind keine Methoden für die erneute Aushandlung oder Alternative Authentifizierung möglich.

Speicherort:%windir%\windows\system32\negoexs.dll

Dieser Anbieter ist standardmäßig in Versionen enthalten, die in der Liste **gilt für** am Anfang dieses Themas angegeben sind, ausgenommen Windows Server 2008 und Windows Vista.

PKU2U Security Support Provider

Das PKU2U-Protokoll wurde in Windows 7 und Windows Server 2008 R2 als SSP eingeführt und implementiert. Dieser SSP ermöglicht die Peer-zu-Peer-Authentifizierung, insbesondere über das Medien- und Dateifreigabe Feature namens HomeGroup, das in Windows 7 eingeführt wurde. Die Funktion ermöglicht die Freigabe von Computern, die nicht Mitglied einer Domäne sind.

Speicherort:%windir%\windows\system32\pku2u.dll

Dieser Anbieter ist standardmäßig in Versionen enthalten, die in der Liste **gilt für** am Anfang dieses Themas angegeben sind, ausgenommen Windows Server 2008 und Windows Vista.

Zusätzliche Ressourcen für das PKU2U-Protokoll und den PKU2U SSP

- [Einführung in die Online-Identitäts Integration](#)

Auswahl des Sicherheits Unterstützungs Anbieters

Die Windows-SSPI kann jedes der Protokolle verwenden, die von den installierten Sicherheits Unterstützungs Anbietern unterstützt werden. Da jedoch nicht alle Betriebssysteme dieselben SSP-Pakete unterstützen wie ein beliebiger Computer, auf dem Windows Server ausgeführt wird, müssen Clients und Server die Verwendung eines Protokolls aushandeln, das beide unterstützen. Windows Server bevorzugt Client Computer und Anwendungen für die Verwendung des Kerberos-Protokolls, ein leistungsstarkes Standard basiertes Protokoll, wenn möglich, das Betriebssystem jedoch weiterhin Client Computern und Client Anwendungen, von denen das Kerberos-Protokoll nicht unterstützt wird, zu authentifizieren.

Bevor die Authentifizierung erfolgen kann, müssen die beiden kommunizierenden Computer einem Protokoll zustimmen, das beide unterstützen können. Damit jedes Protokoll über die SSPI verwendbar ist, muss jeder Computer über die entsprechende SSP verfügen. Damit ein Client Computer und ein Server das Kerberos-Authentifizierungsprotokoll verwenden können, müssen beide beispielsweise Kerberos V5 unterstützen. Windows Server verwendet die Funktion " **enumratesecuritypackages** ", um zu ermitteln, welche SSPs auf einem Computer unterstützt werden und welche Funktionen diese SSPs haben.

Die Auswahl eines Authentifizierungs Protokolls kann auf eine der beiden folgenden Arten erfolgen:

1. [Einzelnes Authentifizierungsprotokoll](#)
2. [Aushandeln \(Option\)](#)

Einzelnes Authentifizierungsprotokoll

Wenn ein einzelnes akzeptables Protokoll auf dem Server angegeben ist, muss der Client Computer das angegebene Protokoll unterstützen, oder die Kommunikation schlägt fehl. Wenn ein einzelnes akzeptables Protokoll angegeben wird, erfolgt der Authentifizierungs Austausch wie folgt:

1. Der Client Computer fordert den Zugriff auf einen Dienst an.
2. Der Server antwortet auf die Anforderung und gibt das Protokoll an, das verwendet wird.
3. Der Client Computer überprüft den Inhalt der Antwort und überprüft, ob er das angegebene Protokoll unterstützt. Wenn der Client Computer das angegebene Protokoll unterstützt, wird die Authentifizierung fortgesetzt. Wenn der Client Computer das Protokoll nicht unterstützt, schlägt die Authentifizierung fehl, unabhängig davon, ob der Client Computer für den Zugriff auf die Ressource autorisiert ist.

Aushandeln (Option)

Die Option aushandeln kann verwendet werden, um dem Client und dem Server zu ermöglichen, ein akzeptables Protokoll zu finden. Dies basiert auf dem einfachen und geschützten GSS-API-Aushandlungs Mechanismus (spnetgo). Wenn die Authentifizierung mit der Option zum Aushandeln eines Authentifizierungs Protokolls beginnt, erfolgt der spnetgo-Austausch wie folgt:

1. Der Client Computer fordert den Zugriff auf einen Dienst an.
2. Der Server antwortet mit einer Liste von Authentifizierungs Protokollen, die er unterstützen kann, sowie einer Authentifizierungs Aufforderung oder-Antwort, die auf dem Protokoll basiert, das die erste Wahl ist. Der Server kann z. b. das Kerberos-Protokoll und NTLM auflisten und eine Kerberos-Authentifizierungs Antwort senden.
3. Der Client Computer überprüft den Inhalt der Antwort und überprüft, ob er eines der angegebenen Protokolle unterstützt.
 - Wenn der Client Computer das bevorzugte Protokoll unterstützt, wird die Authentifizierung fortgesetzt.
 - Wenn der Client Computer das bevorzugte Protokoll nicht unterstützt, aber eines der anderen vom Server aufgelisteten Protokolle unterstützt, kann der Server vom Client Computer wissen, welches Authentifizierungsprotokoll unterstützt wird, und die Authentifizierung wird durchgeführt.
 - Wenn der Client Computer keines der aufgelisteten Protokolle unterstützt, schlägt der Authentifizierungs Austausch fehl.

Siehe auch

[Architektur der Windows-Authentifizierung](#)

Anmeldeinformationen-Prozesse in der Windows-Authentifizierung

09.04.2020 • 53 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

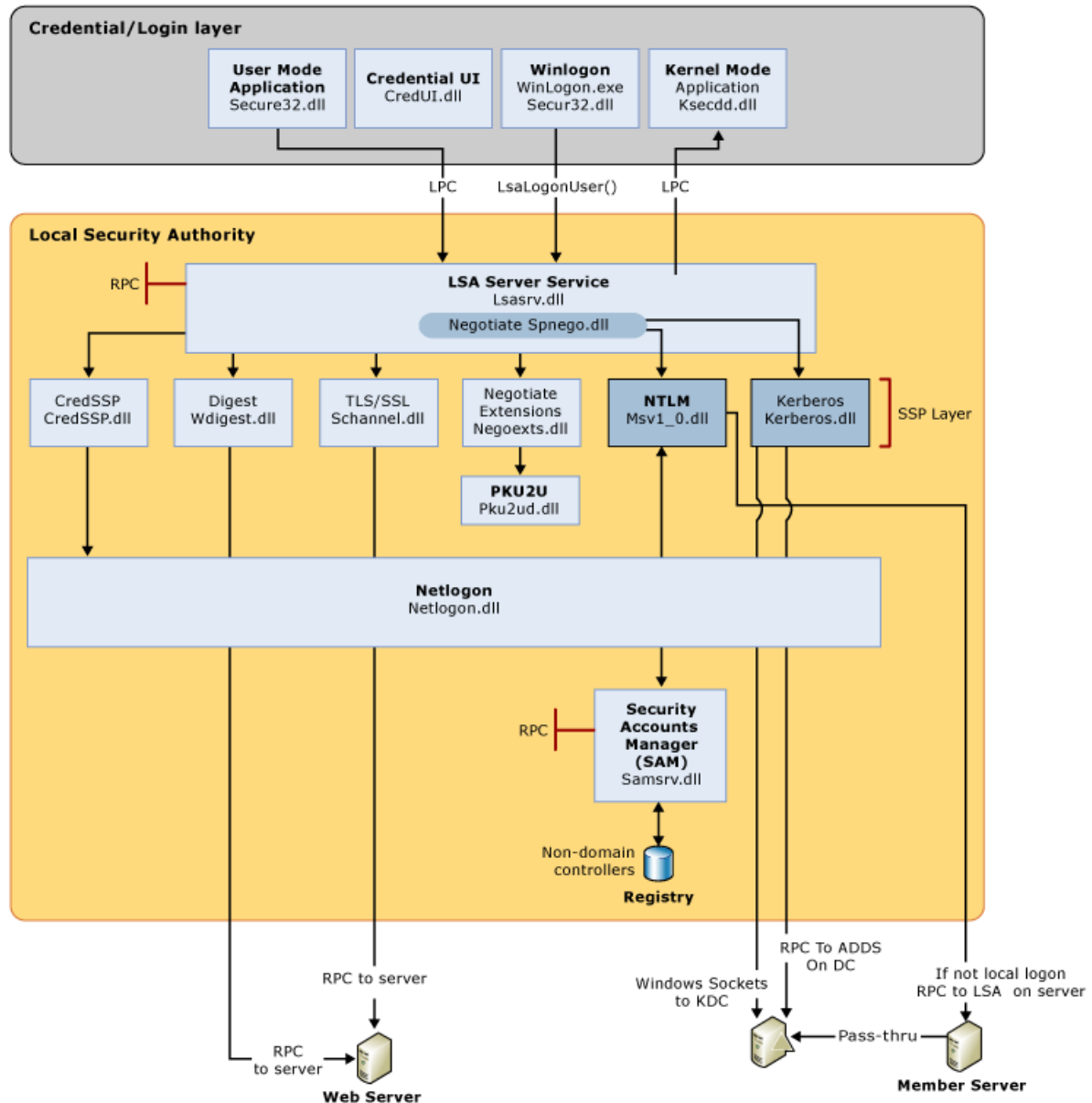
In diesem Referenz Thema für IT-Experten wird beschrieben, wie die Windows-Authentifizierung Anmelde Informationen verarbeitet.

Bei der Verwaltung von Windows-Anmelde Informationen handelt es sich um den Prozess, mit dem das Betriebssystem die Anmelde Informationen vom Dienst oder Benutzer empfängt und diese Informationen für die zukünftige Präsentation des authentifizier enden Ziels sichert. Bei einem Computer, der einer Domäne beigetreten ist, ist das authentifizier Ende Ziel der Domänen Controller. Die Anmelde Informationen, die bei der Authentifizierung verwendet werden, sind digitale Dokumente, die die Identität des Benutzers einer Art von Echtheit zuweisen, z. b. ein Zertifikat, ein Kennwort oder eine PIN.

Standardmäßig werden Windows-Anmelde Informationen anhand der SAM-Datenbank (Security Accounts Manager) auf dem lokalen Computer oder mit Active Directory auf einem in die Domäne eingebundenen Computer über den Winlogon-Dienst überprüft. Anmelde Informationen werden über Benutzereingaben auf der Anmelde Benutzeroberfläche oder Programm gesteuert über die Anwendungsprogrammierschnittstelle (Application Programming Interface, API) erfasst, die dem authentifizier enden Ziel angezeigt werden.

Lokale Sicherheitsinformationen werden in der Registrierung unter **HKEY_LOCAL_MACHINE \Security** gespeichert. Zu den gespeicherten Informationen gehören Richtlinien Einstellungen, Standard Sicherheitswerte und Kontoinformationen, wie z. b. zwischengespeicherte Anmelde Informationen. Hier wird auch eine Kopie der SAM-Datenbank gespeichert, obwohl sie schreibgeschützt ist.

Das folgende Diagramm zeigt die erforderlichen Komponenten und die Pfade, die von den Anmelde Informationen über das System übernommen werden, um den Benutzer oder den Prozess für eine erfolgreiche Anmeldung zu authentifizieren.



In der folgenden Tabelle werden die einzelnen Komponenten beschrieben, mit denen Anmelde Informationen im Authentifizierungsprozess zum Zeitpunkt der Anmeldung verwaltet werden.

Authentifizierungs Komponenten für alle Systeme

| KOMPONENTE | BESCHREIBUNG |
|------------------------|---|
| Anmelden des Benutzers | Winlogon.exe ist die ausführbare Datei, die für die Verwaltung sicherer Benutzerinteraktionen zuständig ist. Der Winlogon-Dienst initiiert den Anmeldevorgang für Windows-Betriebssysteme, indem er die von der Benutzeraktion gesammelten Anmelde Informationen auf dem sicheren Desktop (Anmelde Benutzeroberfläche) über Secur32.dll an die lokale Sicherheits Autorität (Local Security Authority, LSA) übergibt. |

| KOMPONENTE | BESCHREIBUNG |
|---------------------------------------|---|
| Anwendungs Anmeldung | <p>Anwendungs-oder Dienst Anmeldungen, die keine interaktive Anmeldung erfordern. Die meisten vom Benutzer initiierten Prozesse werden mithilfe von Secur32.dll im Benutzermodus ausgeführt, während Prozesse, die beim Start initiiert werden, wie z. B. Dienste, mithilfe von Ksecdd.sys im Kernel Modus ausgeführt werden.</p> <p>Weitere Informationen zum Benutzermodus und Kernel Modus finden Sie unter Anwendungen und Benutzermodus oder Dienste und Kernel Modus in diesem Thema.</p> |
| Secur32.dll | Die Anbieter für mehrfache Authentifizierung, die die Grundlage für den Authentifizierungsprozess bilden. |
| Lsasrv.dll | Der LSA-Server Dienst, der beide Sicherheitsrichtlinien erzwingt und als Sicherheitspaket-Manager für die LSA fungiert. Die LSA enthält die Funktion "aushandeln", die das NTLM-oder Kerberos-Protokoll auswählt, nachdem ermittelt wurde, welches Protokoll erfolgreich sein soll. |
| Anbieter für Sicherheitsunterstützung | Eine Gruppe von Anbietern, die ein oder mehrere Authentifizierungsprotokolle einzeln aufrufen können. Der Standardsatz von Anbietern kann sich mit jeder Version des Windows-Betriebssystems ändern, und es können benutzerdefinierte Anbieter geschrieben werden. |
| Netlogon.dll | <p>Die vom Anmelde Dienst ausgeführten Dienste lauten wie folgt:</p> <ul style="list-style-type: none"> : Verwaltet den sicheren Kanal des Computers (nicht zu verwechseln mit SChannel) mit einem Domänen Controller. : Übergibt die Anmelde Informationen des Benutzers über einen sicheren Kanal an den Domänen Controller und gibt die Domänen Sicherheits-IDs (SIDs) und Benutzerrechte für den Benutzer zurück. : Veröffentlicht Dienst Ressourcen Einträge im Domain Name System (DNS) und verwendet DNS, um Namen in die IP-Adressen von Domänen Controllern aufzulösen. : Implementiert das Replikations Protokoll auf der Grundlage von Remote Prozedur Aufruf (RPC) zum Synchronisieren von primären Domänen Controllern (PDCs) und Sicherungs Domänen Controllern (BDCs). |
| Samsrv.dll | Der Security Accounts Manager (Sam), der lokale Sicherheits Konten speichert, erzwingt lokal gespeicherte Richtlinien und unterstützt APIs. |
| Registrierung | Die Registrierung enthält eine Kopie der SAM-Datenbank, Einstellungen für lokale Sicherheitsrichtlinien, Standard Sicherheitswerte und Kontoinformationen, die nur für das System zugänglich sind. |

Dieses Thema enthält folgende Abschnitte:

- [Eingabe der Anmelde Informationen für die Benutzeranmeldung](#)
- [Eingabe der Anmelde Informationen für die Anmeldung von Anwendungen und Diensten](#)

- Lokale Sicherheits Autorität
- Zwischengespeicherte Anmelde Informationen und Validierung
- Speicherung und Validierung von Anmelde Informationen
- Sicherheits Konten-Manager-Datenbank
- Lokale Domänen und vertrauenswürdige Domänen
- Zertifikate in der Windows-Authentifizierung

Eingabe der Anmelde Informationen für die Benutzeranmeldung

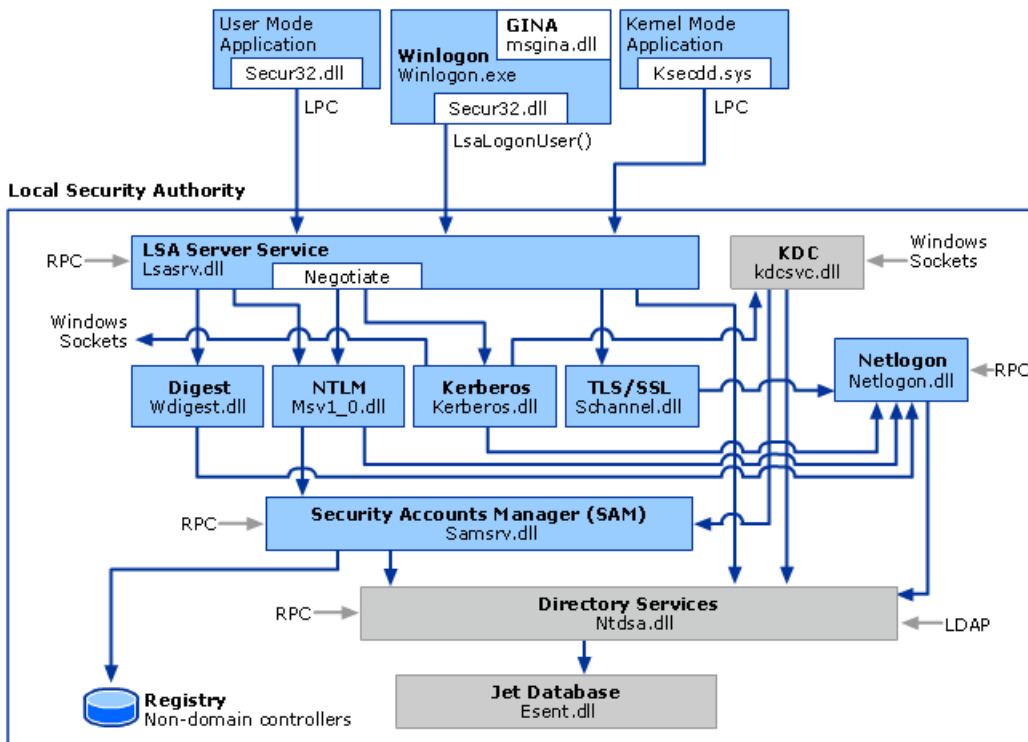
In Windows Server 2008 und Windows Vista wurde die Gina-Architektur (Graphical Identification and Authentication) durch ein Anmelde Informationsanbieter-Modell ersetzt, das es ermöglicht, unterschiedliche Anmelde Typen durch die Verwendung von Anmelde Kacheln aufzuzählen. Beide Modelle werden unten beschrieben.

Grafische Identifizierungs-und Authentifizierungs Architektur

Die Graphical Identification and Authentication (Gina)-Architektur gilt für die Betriebssysteme Windows Server 2003, Microsoft Windows 2000 Server, Windows XP und Windows 2000 Professional. In diesen Systemen erstellt jede interaktive Anmelde Sitzung eine separate Instanz des Winlogon-Diensts. Die Gina-Architektur wird in den von Winlogon verwendeten Prozessbereich geladen, empfängt und verarbeitet die Anmelde Informationen und führt die Aufrufe der Authentifizierungs Schnittstellen über LsaLogonUser durch.

Die Instanzen von Winlogon für eine interaktive Anmeldung werden in Sitzung 0 ausgeführt. Sitzung 0 hostet Systemdienste und andere kritische Prozesse, einschließlich des LSA-Prozesses (Local Security Authority, lokale Sicherheits Autorität).

Das folgende Diagramm zeigt den Anmelde Informationsprozess für Windows Server 2003, Microsoft Windows 2000 Server, Windows XP und Microsoft Windows 2000 Professional.



Architektur des Anmelde Informationsanbieters

Die Anmelde Informationsanbieter-Architektur gilt für die Versionen, die in der Liste **gilt für** am Anfang dieses Themas angegeben sind. In diesen Systemen wurde die Eingabe Architektur der Anmelde Informationen mithilfe

von Anmelde Informationsanbietern in einen erweiterbaren Entwurf geändert. Diese Anbieter werden durch die verschiedenen Anmelde Kacheln auf dem sicheren Desktop dargestellt, die eine beliebige Anzahl von Anmelde Szenarios zulassen: verschiedene Konten für denselben Benutzer und verschiedene Authentifizierungsmethoden, z. b. Kennwort, Smartcard und Biometrie.

Bei der Architektur des Anmelde Informationsanbieters startet Winlogon immer die Anmelde Benutzeroberfläche, nachdem Sie ein sicheres Ereignis für die Ereignis Ereignis Erstellung erhalten hat. Anmelde Benutzeroberfläche fragt jeden Anmelde Informationsanbieter für die Anzahl unterschiedlicher Anmelde Informationstypen ab, für die der Anbieter für die Aufzählung konfiguriert ist. Anmelde Informationsanbieter haben die Möglichkeit, eine dieser Kacheln als Standard anzugeben. Nachdem alle Anbieter Ihre Kacheln aufgezählt haben, werden Sie von der Anmelde Benutzeroberfläche dem Benutzer angezeigt. Der Benutzer interagiert mit einer Kachel, um seine Anmelde Informationen anzugeben. Die Anmelde Benutzeroberfläche übermittelt diese Anmelde Informationen zur Authentifizierung.

Anmelde Informationsanbieter sind keine Erzwingungs Mechanismen. Sie werden verwendet, um Anmelde Informationen zu erfassen und zu serialisieren. Die lokale Sicherheits Autorität und die Authentifizierungs Pakete erzwingen die Sicherheit.

Anmelde Informationsanbieter werden auf dem Computer registriert und sind für Folgendes verantwortlich:

- Beschreiben der Anmelde Informationen, die für die Authentifizierung erforderlich sind.
- Verarbeiten von Kommunikation und Logik mit externen Authentifizierungs stellen.
- Verpacken von Anmelde Informationen für die interaktive und die Netzwerk Anmeldung.

Das Verpacken von Anmelde Informationen für die interaktive und Netzwerk Anmeldung schließt den Prozess der Serialisierung ein. Durch das Serialisieren von Anmelde Informationen können mehrere Anmelde Kacheln auf der Anmelde Benutzeroberfläche angezeigt werden. Aus diesem Grund kann Ihre Organisation die Anmelde Anzeige steuern, z. b. Benutzer, Zielsysteme für die Anmeldung, Zugriff vor der Anmeldung auf das Netzwerk und Richtlinien zum Sperren/Entsperren von Richtlinien durch Verwendung von angepassten Anmelde Informationsanbietern. Mehrere Anmelde Informationsanbieter können auf demselben Computer nebeneinander vorhanden sein.

Anbieter für einmaliges Anmelden (Single Sign-on, SSO) können als Standard Anmelde Informationsanbieter oder als Pre-Logon-Access-Anbieter entwickelt werden.

Jede Version von Windows enthält einen standardmäßigen Anmelde Informationsanbieter und einen standardmäßigen Pre-Logon-Access-Anbieter (PLAP), der auch als SSO-Anbieter bezeichnet wird. Der SSO-Anbieter ermöglicht es Benutzern, eine Verbindung mit einem Netzwerk herzustellen, bevor Sie sich beim lokalen Computer anmelden. Wenn dieser Anbieter implementiert ist, listet der Anbieter keine Kacheln auf der Anmelde Benutzeroberfläche auf.

Ein SSO-Anbieter sollte in den folgenden Szenarien verwendet werden:

- **Netzwerk Authentifizierung und Computer Anmeldung werden von verschiedenen Anmelde Informationsanbietern verarbeitet.** Zu den Abweichungen dieses Szenarios gehören:
 - Ein Benutzer hat die Möglichkeit, eine Verbindung mit einem Netzwerk herzustellen, z. b. das Herstellen einer Verbindung mit einem virtuellen privaten Netzwerk (VPN), bevor er sich beim Computer anmeldet, jedoch nicht für diese Verbindung benötigt wird.
 - Zum Abrufen von Informationen, die während der interaktiven Authentifizierung auf dem lokalen Computer verwendet werden, ist eine Netzwerk Authentifizierung erforderlich.
 - Auf mehrere Netzwerk Authentifizierungen folgt eines der anderen Szenarien. Ein Benutzer authentifiziert sich beispielsweise bei einem Internet Dienstanbieter (Internet Service Provider, ISP), authentifiziert sich bei einem VPN und verwendet dann seine Anmelde Informationen für das

Benutzerkonto, um sich lokal anzumelden.

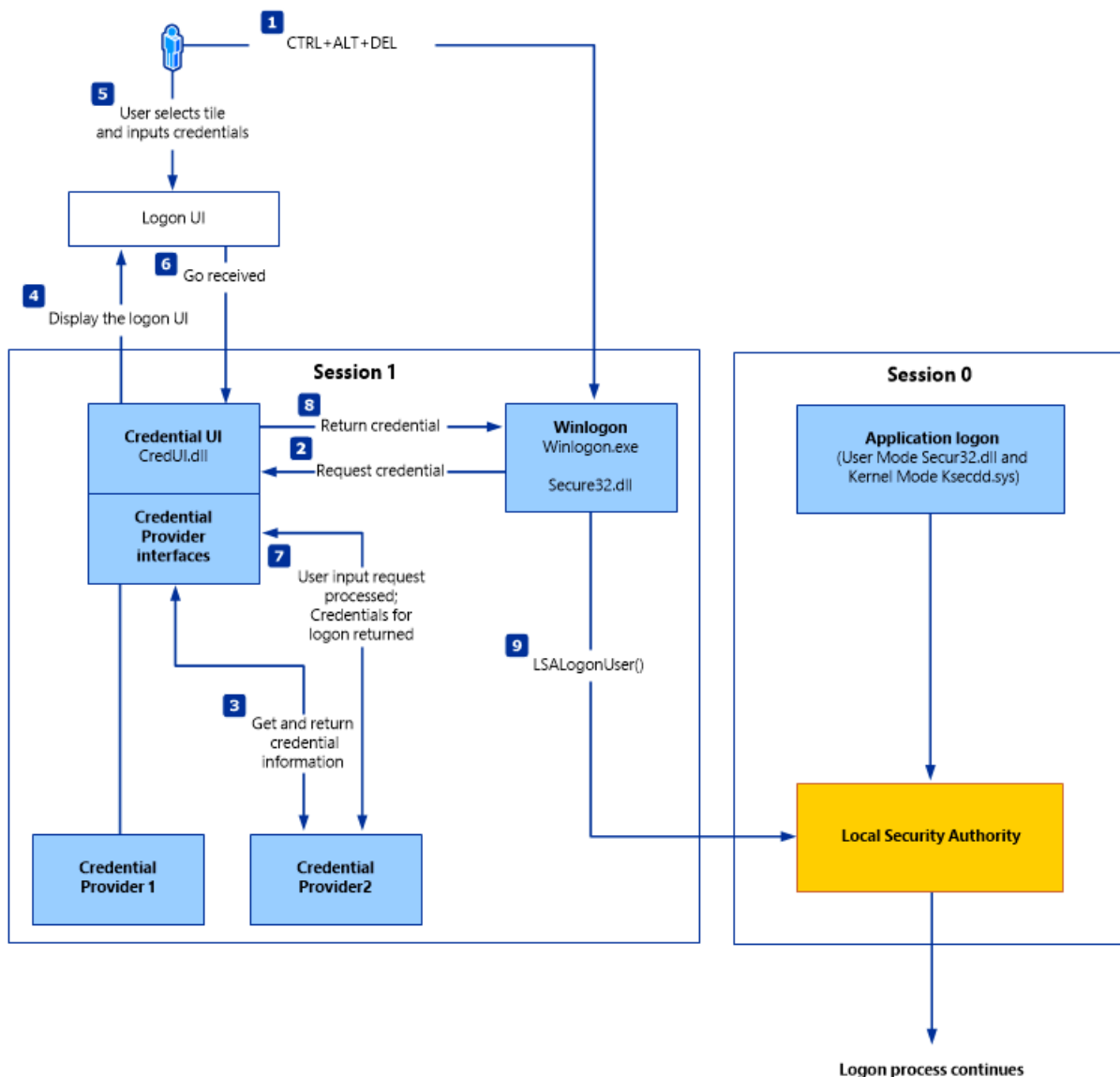
- Zwischengespeicherte Anmelde Informationen sind deaktiviert, und vor der lokalen Anmeldung ist eine Remote Zugriffs Dienste-Verbindung über VPN erforderlich, um den Benutzer zu authentifizieren.
- Ein Domänen Benutzer verfügt über kein lokales Konto, das auf einem in die Domäne eingebundenen Computer eingerichtet wurde, und muss vor dem Abschließen der interaktiven Anmeldung eine Remote Zugriffs Dienste-Verbindung über eine VPN-Verbindung herstellen.
- **Netzwerk Authentifizierung und Computer Anmeldung werden vom gleichen Anmelde Informationsanbieter verarbeitet.** In diesem Szenario muss der Benutzer eine Verbindung mit dem Netzwerk herstellen, bevor er sich beim Computer anmelden kann.

Anmelde Kachel-Enumeration

Der Anmelde Informationsanbieter listet die Anmelde Kacheln in den folgenden Instanzen auf:

- Für die Betriebssysteme, die in der Liste **gilt für** am Anfang dieses Themas angegeben sind.
- Der Anmelde Informationsanbieter listet die Kacheln für die Arbeitsstations Anmeldung auf. Der Anmelde Informationsanbieter serialisiert in der Regel Anmelde Informationen für die Authentifizierung bei der lokalen Sicherheits Autorität. Bei diesem Vorgang werden für jeden benutzerspezifische Kacheln angezeigt, die für die Zielsysteme der einzelnen Benutzer spezifisch sind.
- Mit der Anmelde-und Authentifizierungs Architektur kann ein Benutzer Kacheln verwenden, die vom Anmelde Informationsanbieter aufgelistet werden, um eine Arbeitsstation zu entsperren. In der Regel ist der aktuell angemeldete Benutzer die Standard Kachel, aber wenn mehr als ein Benutzer angemeldet ist, werden zahlreiche Kacheln angezeigt.
- Der Anmelde Informationsanbieter listet Kacheln als Reaktion auf eine Benutzer Anforderung auf, um Ihr Kennwort oder andere private Informationen, wie z. b. eine PIN, zu ändern. In der Regel ist der aktuell angemeldete Benutzer die Standard Kachel. Wenn jedoch mehr als ein Benutzer angemeldet ist, werden zahlreiche Kacheln angezeigt.
- Der Anmelde Informationsanbieter listet Kacheln auf der Grundlage der serialisierten Anmelde Informationen auf, die für die Authentifizierung auf Remote Computern verwendet werden sollen. Die Benutzeroberfläche für Anmelde Informationen verwendet nicht die gleiche Instanz des Anbieters wie die Anmelde Benutzeroberfläche, die Sperre für die Arbeitsstation oder das Ändern des Kennworts. Daher können Zustandsinformationen im Anbieter zwischen Instanzen der Benutzeroberfläche für Anmelde Informationen nicht beibehalten werden. Diese Struktur ergibt eine Kachel für jede Remote Computer Anmeldung, vorausgesetzt, dass die Anmelde Informationen ordnungsgemäß serialisiert wurden. Dieses Szenario wird auch in der Benutzerkontensteuerung (User Account Control, UAC) verwendet, die dazu beiträgt, nicht autorisierte Änderungen an einem Computer zu verhindern, indem der Benutzer aufgefordert wird, Berechtigungen oder ein Administrator Kennwort einzugeben, bevor er Aktionen zulässt, die sich potenziell auf den Betrieb des Computers auswirken könnten oder Einstellungen ändern können, die andere Benutzer des Computers betreffen

Das folgende Diagramm zeigt den Anmelde Informationsprozess für die Betriebssysteme, die in der Liste **gilt für** am Anfang dieses Themas angegeben sind.



Eingabe der Anmelde Informationen für die Anmeldung von Anwendungen und Diensten

Die Windows-Authentifizierung dient zum Verwalten von Anmelde Informationen für Anwendungen oder Dienste, für die keine Benutzerinteraktion erforderlich ist. Anwendungen im Benutzermodus sind auf die Systemressourcen beschränkt, auf die Sie Zugriff haben, während Dienste uneingeschränkten Zugriff auf den Systemspeicher und externe Geräte haben können.

System Dienste und Anwendungen auf Transport Ebene greifen über die Security Support Provider-Schnittstelle (SSPI) in Windows auf einen Security Support Provider (SSP) zu, der Funktionen zum Auflisten der auf einem System verfügbaren Sicherheitspakete, zum Auswählen eines Pakets und zum Verwenden dieses Pakets zum Abrufen einer authentifizierten Verbindung bereitstellt.

Wenn eine Client/Server-Verbindung authentifiziert wird:

- Die Anwendung auf der Clientseite der Verbindung sendet mithilfe der SSPI-Funktion `InitializeSecurityContext (General)` Anmelde Informationen an den Server.
- Die Anwendung auf der Serverseite der Verbindung antwortet mit der SSPI-Funktion `AcceptSecurityContext (General)`.
- Die SSPI-Funktionen `InitializeSecurityContext (General)` und `AcceptSecurityContext (General)` werden wiederholt, bis alle erforderlichen Authentifizierungs Nachrichten zur erfolgreichen oder fehlerhaften Authentifizierung ausgetauscht wurden.

- Nachdem die Verbindung authentifiziert wurde, werden von der LSA auf dem Server Informationen vom Client verwendet, um den Sicherheitskontext zu erstellen, der ein Zugriffs Token enthält.
- Der Server kann dann die SSPI-Funktion `ImpersonateSecurityContext` aufrufen, um das Zugriffs Token an einen Identitätswechsel Thread für den Dienst anzufügen.

Anwendungen und Benutzermodus

Der Benutzermodus in Windows besteht aus zwei Systemen, die e/a-Anforderungen an die entsprechenden Kernelmodustreiber übergeben können: das Umgebungs System, das Anwendungen ausführt, die für viele verschiedene Betriebssystem Typen geschrieben wurden, und das integrale System, das systemspezifische Funktionen im Namen des Umgebungs Systems betreibt.

Das integrale System verwaltet betriebssystemspezifische Funktionen im Namen des Umgebungs Systems und besteht aus einem Sicherheitssystem Prozess (LSA), einem Arbeitsstations Dienst und einem Server Dienst. Der Sicherheitssystem Prozess behandelt Sicherheits Token, erteilt oder verweigert Berechtigungen für den Zugriff auf Benutzerkonten auf der Grundlage von Ressourcen Berechtigungen, verarbeitet Anmelde Anforderungen und initiiert die Anmelde Authentifizierung und bestimmt, welche Systemressourcen das Betriebssystem überwachen muss.

Anwendungen können im Benutzermodus ausgeführt werden, in dem die Anwendung als beliebiger Prinzipal ausgeführt werden kann, einschließlich im Sicherheitskontext des lokalen Systems (System). Anwendungen können auch im Kernel Modus ausgeführt werden, in dem die Anwendung im Sicherheitskontext des lokalen Systems (System) ausgeführt werden kann.

SSPI steht über das Modul Secur32.dll zur Verfügung, das eine API zum Abrufen integrierter Sicherheitsdienste für Authentifizierung, Nachrichten Integrität und Nachrichten Datenschutz ist. Es stellt eine Abstraktions Ebene zwischen Protokollen auf Anwendungsebene und Sicherheitsprotokollen bereit. Da für verschiedene Anwendungen unterschiedliche Methoden zum identifizieren oder Authentifizieren von Benutzern und zum Verschlüsseln von Daten während der Übertragung über ein Netzwerk erforderlich sind, bietet SSPI eine Möglichkeit für den Zugriff auf DLLs (Dynamic-Link Libraries), die unterschiedliche Authentifizierungs- und Kryptografiefunktionen enthalten. Diese DLLs werden als Security Support Provider (SSPs) bezeichnet.

Verwaltete Dienst Konten und virtuelle Konten wurden in Windows Server 2008 R2 und Windows 7 eingeführt, um wichtige Anwendungen, wie z. b. Microsoft SQL Server und Internetinformationsdienste (IIS), mit der Isolation ihrer eigenen Domänen Konten bereitzustellen. gleichzeitig entfällt die Notwendigkeit, dass ein Administrator den Dienst Prinzipal Namen (SPN) und die Anmelde Informationen für diese Konten manuell verwaltet. Weitere Informationen zu diesen Features und deren Rolle bei der Authentifizierung finden Sie in der [Dokumentation zu verwalteten Dienst Konten für Windows 7 und Windows Server 2008 R2](#) und [Übersicht über Gruppen verwaltete Dienst Konten](#).

Dienste und Kernel Modus

Obwohl die meisten Windows-Anwendungen im Sicherheitskontext des Benutzers ausgeführt werden, der Sie startet, gilt dies nicht für die Dienste. Viele Windows-Dienste, z. b. Netzwerk- und Druckdienste, werden vom Dienst Controller gestartet, wenn der Benutzer den Computer startet. Diese Dienste können als lokaler Dienst oder lokales System ausgeführt werden und werden möglicherweise weiterhin ausgeführt, nachdem sich der letzte Benutzer abgemeldet hat.

NOTE

Dienste werden normalerweise in Sicherheits Kontexten ausgeführt, die als lokales System (System), Netzwerkdienst oder lokaler Dienst bezeichnet werden. Windows Server 2008 R2 hat Dienste eingeführt, die unter einem verwalteten Dienst Konto ausgeführt werden, bei dem es sich um Domänen Prinzipale handelt.

Vor dem Starten eines dienststanders meldet sich der Dienst Controller mit dem Konto an, das für den Dienst

bestimmt ist, und zeigt dann die Anmelde Informationen des Dienstanbieter für die Authentifizierung durch die LSA an. Der Windows-Dienst implementiert eine programmgesteuerte Schnittstelle, mit der der Service Controller-Manager den Dienst steuern kann. Ein Windows-Dienst kann automatisch gestartet werden, wenn das System gestartet oder manuell mit einem Dienst Steuerungsprogramm gestartet wird. Wenn ein Windows-Client Computer z. b. einer Domäne Beitritt, stellt der Messenger-Dienst auf dem Computer eine Verbindung mit einem Domänen Controller her und öffnet einen sicheren Kanal. Zum Abrufen einer authentifizierten Verbindung muss der Dienst über Anmelde Informationen verfügen, denen die lokale Sicherheits Autorität (LSA) des Remote Computers vertraut. Bei der Kommunikation mit anderen Computern im Netzwerk werden von der LSA die Anmelde Informationen für das Domänen Konto des lokalen Computers verwendet, ebenso wie alle anderen Dienste, die im Sicherheitskontext des lokalen Systems und des Netzwerk Diensts ausgeführt werden. Dienste auf dem lokalen Computer werden als System ausgeführt, sodass keine Anmelde Informationen für die LSA angezeigt werden müssen.

Diese Anmelde Informationen werden von der Datei "Ksecdd. sys" verwaltet und verschlüsselt, und es wird ein lokaler Prozedur Aufrufe in die LSA verwendet. Der Dateityp ist "drv (Driver)" und wird als SSP (Kernel Mode Security Support Provider) bezeichnet, und in den Versionen, die in der Liste **gilt für** am Anfang dieses Themas angegeben sind, ist "fps 140-2 Level 1-kompatibel".

Der Kernel Modus verfügt über Vollzugriff auf die Hardware-und Systemressourcen des Computers. Der Kernel Modus hindert benutzermodusdienste und-Anwendungen daran, auf kritische Bereiche des Betriebssystems zuzugreifen, auf die Sie keinen Zugriff haben sollen.

Lokale Sicherheits Autorität

Bei der lokalen Sicherheits Autorität (Local Security Authority, LSA) handelt es sich um einen geschützten System Prozess, der Benutzer auf dem lokalen Computer authentifiziert und protokolliert. Außerdem verwaltet LSA Informationen über alle Aspekte der lokalen Sicherheit auf einem Computer (diese Aspekte werden zusammen als lokale Sicherheitsrichtlinie bezeichnet) und bietet verschiedene Dienste für die Übersetzung zwischen Namen und Sicherheits-IDs (SIDs). Der Sicherheitssystem Prozess (Local Security Authority Server Service, LSASS) verfolgt die Sicherheitsrichtlinien und die Konten, die auf einem Computersystem wirksam sind.

Die LSA überprüft die Identität eines Benutzers, je nachdem, welche der folgenden beiden Entitäten das Konto des Benutzers ausgegeben hat:

- **Lokale Sicherheits Autorität.** Die LSA kann Benutzerinformationen überprüfen, indem Sie die SAM-Datenbank (Security Accounts Manager) auf demselben Computer überprüfen. Auf allen Arbeitsstationen und Mitglieds Servern können lokale Benutzerkonten und Informationen zu lokalen Gruppen gespeichert werden. Diese Konten können jedoch nur für den Zugriff auf diese Arbeitsstation oder den Computer verwendet werden.
- **Sicherheits Autorität für die lokale Domäne oder für eine vertrauenswürdige Domäne.** Die LSA kontaktiert die Entität, die das Konto ausgestellt hat, und fordert die Überprüfung an, dass das Konto gültig ist und die Anforderung vom Kontoinhaber stammt.

Der Subsystemdienst für die lokale Sicherheitsautorität (Local Security Authority Subsystem Service, LSASS) speichert Anmeldeinformationen für Benutzer mit aktiven Windows-Sitzungen im Arbeitsspeicher. Mit den gespeicherten Anmelde Informationen können Benutzer nahtlos auf Netzwerkressourcen wie Dateifreigaben, Exchange Server-Postfächer und SharePoint-Websites zugreifen, ohne Ihre Anmelde Informationen für jeden Remote Dienst erneut eingeben zu müssen.

LSASS kann Anmeldeinformationen in verschiedenen Formaten speichern. Diese umfassen Folgendes:

- Reversibel verschlüsselter Nur-Text
- Kerberos-Tickets (Ticket-Tickets (TGTs), Dienst Tickets)
- NT-Hash

- LAN-Manager (LM)-Hash

Wenn sich der Benutzer unter Verwendung einer Smartcard bei Windows anmeldet, speichert LSASS kein nur-Text-Kennwort, sondern speichert den entsprechenden NT-Hashwert für das Konto und die nur-Text-PIN für die Smartcard. Wenn das Kontoattribut für eine Smartcard aktiviert ist, die für die interaktive Anmeldung erforderlich ist, wird für das Konto automatisch ein zufälliger NT-Hashwert anstelle des ursprünglichen Kennworthashes generiert. Der automatisch beim Festlegen des Attributs generierte Kennworthash wird nicht geändert.

Wenn sich ein Benutzer bei einem Windows-basierten Computer mit einem Kennwort anmeldet, das mit dem LAN-Manager (LM)-Hashes kompatibel ist, ist dieser Authentifikator im Arbeitsspeicher vorhanden.

Die Speicherung von Nur-Text-Anmeldeinformationen im Arbeitsspeicher kann nicht deaktiviert werden, auch nicht, wenn die diese Informationen anfordernden Anmeldeinformationsanbieter deaktiviert sind.

Die gespeicherten Anmelde Informationen sind direkt den Anmelde Sitzungen des Subsystemdienst für die lokale Sicherheitsautorität (LSASS) zugeordnet, die nach dem letzten Neustart gestartet und nicht geschlossen wurden. LSA-Sitzungen mit gespeicherten LSA-Anmeldeinformationen werden beispielsweise erstellt, wenn ein Benutzer eine der folgenden Aktionen ausführt:

- Meldet sich bei einer lokalen Sitzung oder einer Remotedesktopprotokoll Sitzung (RDP) auf dem Computer an.
- Ausführen einer Aufgabe mit der Option **RunAs**
- Ausführen eines aktiven Windows-Diensts auf dem Computer
- Ausführen einer geplanten Aufgabe oder eines Batchauftrags
- Ausführen einer Aufgabe auf dem lokalen Computer mithilfe eines Remoteverwaltungstools

In einigen Fällen werden die geheimen Schlüssel der LSA, bei denen es sich um geheime Daten handelt, die nur für System Konto Prozesse zugänglich sind, auf dem Festplattenlaufwerk gespeichert. Einige dieser geheimen Schlüssel sind Anmeldeinformationen, die nach dem Neustart beibehalten werden müssen und verschlüsselt auf dem Festplattenlaufwerk gespeichert werden. Als geheime LSA-Schlüssel gespeicherte Anmeldeinformationen können Folgendes umfassen:

- Konto Kennwort für das Active Directory Domain Services Konto (AD DS) des Computers
- Kontokennwörter für auf dem Computer konfigurierte Windows-Dienste
- Kontokennwörter für konfigurierte geplante Aufgaben
- Kontokennwörter für IIS-Anwendungspools und -Websites
- Kenn Wörter für Microsoft-Konten

Das Client Betriebssystem wurde in Windows 8.1 eingeführt und bietet zusätzlichen Schutz für die LSA, um das Lesen von Arbeitsspeicher und Code Injektion durch nicht geschützte Prozesse zu verhindern. Dieser Schutz erhöht die Sicherheit der Anmelde Informationen, die von der LSA gespeichert und verwaltet werden.

Weitere Informationen zu diesen zusätzlichen Schutzmaßnahmen finden Sie unter [Konfigurieren des zusätzlichen LSA-Schutzes](#).

Zwischengespeicherte Anmelde Informationen und Validierung

Validierungs Mechanismen basieren auf der Präsentation von Anmelde Informationen zum Zeitpunkt der Anmeldung. Wenn der Computer jedoch von einem Domänen Controller getrennt ist und der Benutzer Domänen Anmelde Informationen präsentiert, verwendet Windows den Prozess der zwischengespeicherten Anmelde Informationen im Validierungs Mechanismus.

Jedes Mal, wenn sich ein Benutzer bei einer Domäne anmeldet, speichert Windows die angegebenen Anmelde Informationen zwischen und speichert Sie in der Sicherheitsstruktur in der Registrierung des Betriebssystems.

Mit zwischengespeicherten Anmelde Informationen kann sich der Benutzer bei einem Domänen Mitglied anmelden, ohne dass er mit einem Domänen Controller in dieser Domäne verbunden ist.

Speicherung und Validierung von Anmelde Informationen

Es ist nicht immer wünschenswert, einen Satz von Anmelde Informationen für den Zugriff auf verschiedene Ressourcen zu verwenden. Beispielsweise kann ein Administrator beim Zugriff auf einen Remote Server anstelle von Benutzer Anmelde Informationen Administratorrechte verwenden. Wenn ein Benutzer auf externe Ressourcen (z. b. ein Bankkonto) zugreift, kann er auch nur Anmelde Informationen verwenden, die sich von den Anmelde Informationen der Domäne unterscheiden. In den folgenden Abschnitten werden die Unterschiede bei der Verwaltung von Anmelde Informationen zwischen aktuellen Versionen von Windows-Betriebssystemen und den Betriebssystemen Windows Vista und Windows XP beschrieben.

Remote Anmelde Informationen für Anmelde Informationen

Der Remotedesktopprotokoll (RDP) verwaltet die Anmelde Informationen des Benutzers, der mithilfe des Remotedesktop Clients, der in Windows 8 eingeführt wurde, eine Verbindung mit einem Remote Computer herstellt. Die Anmelde Informationen in Klartext werden an den Zielhost gesendet, auf dem der Host versucht, den Authentifizierungsprozess auszuführen. Wenn der Benutzer erfolgreich ist, wird der Benutzer mit den zulässigen Ressourcen verbunden. RDP speichert die Anmelde Informationen nicht auf dem Client, aber die Domänen Anmelde Informationen des Benutzers werden im LSASS gespeichert.

Der eingeschränkte Administrator Modus wurde in Windows Server 2012 R2 und Windows 8.1 eingeführt und bietet zusätzliche Sicherheit für Remote Anmelde Szenarien. Dieser Modus von Remotedesktop bewirkt, dass die Client Anwendung eine Netzwerk Anmeldeaufforderung mit der unidirektionalen NT-Funktion (ntowf) ausführt oder bei der Authentifizierung beim Remote Host ein Kerberos-Dienst Ticket verwendet. Nachdem der Administrator authentifiziert wurde, verfügt der Administrator nicht über die entsprechenden Konto Anmelde Informationen in LSASS, da diese nicht für den Remote Host bereitgestellt wurden. Stattdessen verfügt der Administrator über die Anmelde Informationen des Computer Kontos für die Sitzung. Administrator Anmelde Informationen werden nicht für den Remote Host bereitgestellt, sodass Aktionen als Computer Konto ausgeführt werden. Ressourcen sind auch auf das Computer Konto beschränkt, und der Administrator kann nicht auf Ressourcen mit seinem eigenen Konto zugreifen.

Automatischer Neustart der Anmelde Informationen für den Anmeldevorgang

Wenn ein Benutzer sich auf einem Windows 8.1 Gerät anmeldet, speichert LSA die Anmelde Informationen des Benutzers in verschlüsseltem Speicher, auf den nur Lsass.exe zugreifen kann. Wenn Windows Update einen automatischen Neustart ohne Benutzer Präsenz initiiert, werden diese Anmelde Informationen verwendet, um die automatische Anmeldung für den Benutzer zu konfigurieren.

Beim Neustart wird der Benutzer automatisch über den Authentifizierungsmechanismus angemeldet, und der Computer wird außerdem zum Schutz der Benutzersitzung gesperrt. Die Sperre wird durch Winlogon initiiert, während die Verwaltung der Anmelde Informationen von LSA erfolgt. Durch automatisches anmelden und Sperren der Sitzung des Benutzers in der-Konsole werden die Anwendungen für den Sperrbildschirm des Benutzers neu gestartet und sind verfügbar.

Weitere Informationen zu ARSO finden Sie [unter Winlogon Automatic Restart Sign-On \(ARSO\)](#).

Gespeicherte Benutzernamen und Kenn Wörter in Windows Vista und Windows XP

In Windows Server 2008, Windows Server 2003, Windows Vista und Windows XP vereinfachen die **gespeicherten Benutzernamen und Kenn Wörter** in der Systemsteuerung die Verwaltung und Verwendung mehrerer Gruppen von Anmelde Informationen, einschließlich X. 509-Zertifikaten, die mit Smartcards und Windows Live-Anmelde Informationen verwendet werden (jetzt als Microsoft-Konto bezeichnet). Die Anmelde Informationen, die Teil des Benutzerprofils sind, werden bis zum Bedarf gespeichert. Durch diese Aktion kann die

Sicherheit auf Ressourcenbasis erhöht werden, indem sichergestellt wird, dass die Sicherheit nicht beeinträchtigt wird, wenn ein Kennwort kompromittiert wird.

Wenn ein Benutzer sich anmeldet und versucht, auf zusätzliche durch Kennwort geschützte Ressourcen wie eine Freigabe auf einem Server zuzugreifen, und wenn die Standard Anmelde Informationen des Benutzers nicht ausreichen, um Zugriff zu erhalten, werden **Gespeicherte Benutzernamen und Kenn Wörter** abgefragt. Wenn Alternative Anmelde Informationen mit den richtigen Anmelde Informationen in **gespeicherten Benutzernamen und Kenn Wörtern** gespeichert wurden, werden diese Anmelde Informationen verwendet, um Zugriff zu erhalten. Andernfalls wird der Benutzer zur Angabe neuer Anmelde Informationen aufgefordert, die dann zur Wiederverwendung gespeichert werden können, entweder später in der Anmelde Sitzung oder während einer nachfolgenden Sitzung.

Die folgenden Einschränkungen gelten:

- Wenn **Gespeicherte Benutzernamen und Kenn Wörter** ungültige oder falsche Anmelde Informationen für eine bestimmte Ressource enthalten, wird der Zugriff auf die Ressource verweigert, und das Dialogfeld **Gespeicherte Benutzernamen und Kenn Wörter** wird nicht angezeigt.
- In **gespeicherten Benutzernamen und Kenn Wörtern** werden Anmelde Informationen nur für NTLM, Kerberos-Protokoll, Microsoft-Konto (früher Windows Live ID) und Secure Sockets Layer (SSL)-Authentifizierung gespeichert. Einige Versionen von Internet Explorer behalten ihren eigenen Cache für die Standard Authentifizierung bei.

Diese Anmelde Informationen werden in das Verzeichnis "\\Dokumente und einstellungen\benutzername\anwendungsdaten\microsoft\benutzername\anwendungsdaten\microsoft\anmelde Informationen" verschlüsselt. Folglich können diese Anmelde Informationen mit dem Benutzer gewechselt werden, wenn die Netzwerk Richtlinie des Benutzers Roamingbenutzerprofile unterstützt. Wenn der Benutzer jedoch Kopien von **gespeicherten Benutzernamen und Kenn Wörtern** auf zwei verschiedenen Computern aufweist und die Anmelde Informationen, die der Ressource auf einem dieser Computer zugeordnet sind, ändert, wird die Änderung nicht an die **gespeicherten Benutzernamen und Kenn Wörter** auf dem zweiten Computer weitergegeben.

Windows Vault und Credential Manager

Die Anmelde Informationsverwaltung wurde in Windows Server 2008 R2 und Windows 7 als System Steuerungsfunktion eingeführt, um Benutzernamen und Kenn Wörter zu speichern und zu verwalten. Mit Credential Manager können Benutzer Anmelde Informationen speichern, die für andere Systeme und Websites im sicheren Windows-Tresor relevant sind. Einige Versionen von Internet Explorer verwenden dieses Feature für die Authentifizierung bei Websites.

Die Verwaltung der Anmeldeinformationen mithilfe der Anmeldeinformationsverwaltung wird durch den Benutzer auf dem lokalen Computer gesteuert. Benutzer können Anmeldeinformationen von unterstützten Browsern und Windows-Anwendungen speichern, um ihnen das erneute Anmelden bei diesen Ressourcen zu erleichtern. Anmelde Informationen werden in speziellen verschlüsselten Ordnern auf dem Computer unter dem Profil des Benutzers gespeichert. Anwendungen, die dieses Feature unterstützen (durch Verwendung der Credential Manager-APIs), z. b. Webbrowser und apps, können während des Anmeldevorgangs anderen Computern und Websites die richtigen Anmelde Informationen zur Verfügung stellen.

Wenn eine Website, eine Anwendung oder ein anderer Computer die Authentifizierung über NTLM oder das Kerberos-Protokoll anfordert, wird ein Dialogfeld angezeigt, in dem Sie das Kontrollkästchen **Standard Anmelde Informationen aktualisieren** oder **Kennwort speichern** auswählen. Dieses Dialogfeld, in dem Benutzer Anmelde Informationen lokal speichern können, wird von einer Anwendung generiert, die die Anmelde Informationsverwaltung-APIs unterstützt. Wenn der Benutzer das Kontrollkästchen **Kennwort speichern** aktiviert, werden der Benutzername, das Kennwort und zugehörige Informationen für den verwendeten Authentifizierungsdienst von Credential Manager nachverfolgt.

Wenn der Dienst das nächste Mal verwendet wird, werden die Anmelde Informationen, die im Windows-Tresor

gespeichert sind, von Anmelde Informationen Manager automatisch bereitgestellt. Werden diese nicht akzeptiert, wird der Benutzer zur Eingabe der richtigen Information für den Zugriff aufgefordert. Wenn der Zugriff mit den neuen Anmelde Informationen gewährt wird, überschreibt die Anmelde Informationsverwaltung die vorherigen Anmelde Informationen mit der neuen Anmelde Information und speichert dann die neuen Anmelde Informationen im Windows-Tresor.

Sicherheits Konten-Manager-Datenbank

Der Security Accounts Manager (Sam) ist eine Datenbank, in der lokale Benutzerkonten und-Gruppen gespeichert werden. Es ist in jedem Windows-Betriebssystem vorhanden. Wenn ein Computer jedoch einer Domäne hinzugefügt wird, verwaltet Active Directory Domänen Konten in Active Directory Domänen.

Beispielsweise werden Client Computer, auf denen ein Windows-Betriebssystem ausgeführt wird, an einer Netzwerk Domäne teilnehmen, indem Sie mit einem Domänen Controller kommunizieren, auch wenn kein Benutzer angemeldet ist. Zum Initiieren der Kommunikation muss der Computer über ein aktives Konto in der Domäne verfügen. Vor dem Akzeptieren der Kommunikation vom Computer wird die Identität des Computers von der LSA auf dem Domänen Controller authentifiziert. Anschließend wird der Sicherheitskontext des Computers genauso wie für einen Human Security Principal erstellt. Dieser Sicherheitskontext definiert die Identität und die Funktionen eines Benutzers oder Diensts auf einem bestimmten Computer, einem Benutzer, einem Dienst oder einem Computer in einem Netzwerk. Das Zugriffs Token, das im Sicherheitskontext enthalten ist, definiert z. b. die Ressourcen (z. b. eine Dateifreigabe oder einen Drucker), auf die zugegriffen werden kann, sowie die Aktionen (z. b. lesen, schreiben oder ändern), die von diesem Prinzipal ausgeführt werden können, einen Benutzer, einen Computer oder einen Dienst für diese Ressource.

Der Sicherheitskontext eines Benutzers oder Computers kann sich von einem Computer zu einem anderen unterscheiden, z. b. wenn sich ein Benutzer an einem Server oder einer anderen Arbeitsstation anmeldet, als die primäre Arbeitsstation des Benutzers. Dies kann auch von einer Sitzung zu einer anderen variieren, z. b. Wenn ein Administrator die Rechte und Berechtigungen des Benutzers ändert. Außerdem ist der Sicherheitskontext in der Regel anders, wenn ein Benutzer oder Computer eigenständig oder in einem Netzwerk oder als Teil einer Active Directory Domäne arbeitet.

Lokale Domänen und vertrauenswürdige Domänen

Wenn eine Vertrauensstellung zwischen zwei Domänen vorhanden ist, basieren die Authentifizierungsmechanismen für jede Domäne auf der Gültigkeit der Authentifizierungen aus der anderen Domäne. Vertrauens Stellungen unterstützen den kontrollierten Zugriff auf freigegebene Ressourcen in einer Ressourcen Domäne (die vertrauende Domäne), indem Sie überprüfen, ob eingehende Authentifizierungsanforderungen von einer vertrauenswürdigen Zertifizierungsstelle (der vertrauenswürdigen Domäne) stammen. Auf diese Weise fungieren Vertrauens Stellungen als Bridges, bei denen nur überprüfte Authentifizierungsanforderungen zwischen Domänen übertragen werden können.

Wie eine bestimmte Vertrauensstellung Authentifizierungsanforderungen übergibt, hängt von der Konfiguration ab. Vertrauens Stellungen können unidirektional sein, indem der Zugriff von der vertrauenswürdigen Domäne auf Ressourcen in der vertrauenden Domäne bereitgestellt wird (oder bidirektional), indem der Zugriff von jeder Domäne auf Ressourcen in der anderen Domäne gewährt wird. Vertrauens Stellungen sind auch nicht transitiv. In diesem Fall besteht nur eine Vertrauensstellung zwischen den beiden vertrauenswürdigen Partner Domänen oder transitiv. In diesem Fall wird eine Vertrauensstellung automatisch auf alle anderen Domänen ausgedehnt, denen beide Partner vertraut sind.

Informationen zu Domänen- und Gesamtstruktur-Vertrauens Stellungen hinsichtlich der Authentifizierung finden Sie unter [Delegierte Authentifizierung und Vertrauensstellungen](#).

Zertifikate in der Windows-Authentifizierung

Bei einer Public Key-Infrastruktur (PKI) handelt es sich um eine Kombination aus Software, Verschlüsselungstechnologien, Prozessen und Diensten, mit deren Hilfe die Kommunikation und Geschäftstransaktionen einer Organisation gesichert werden können. Die Fähigkeit einer PKI zum Sichern von Kommunikation und Geschäftstransaktionen basiert auf dem Austausch digitaler Zertifikate zwischen authentifizierten Benutzern und vertrauenswürdigen Ressourcen.

Ein digitales Zertifikat ist ein elektronisches Dokument, das Informationen über die Entität enthält, zu der es gehört, die von ihm ausgegebene Entität, eine eindeutige Seriennummer oder andere eindeutige Identifikations-, Ausstellungs- und Ablaufdaten sowie einen digitalen Fingerabdruck.

Die Authentifizierung ist der Prozess, bei dem ermittelt wird, ob ein Remote Host vertrauenswürdig ist. Um seine Vertrauenswürdigkeit einzurichten, muss der Remote Host ein akzeptables Authentifizierungszertifikat bereitstellen.

Remote Hosts richten ihre Vertrauenswürdigkeit ein, indem Sie ein Zertifikat von einer Zertifizierungsstelle (Certification Authority, ca) erhalten. Die Zertifizierungsstelle kann wiederum über eine Zertifizierung von einer höheren Zertifizierungsstelle verfügen, die eine Vertrauenskette erstellt. Um zu ermitteln, ob ein Zertifikat vertrauenswürdig ist, muss eine Anwendung die Identität der Stamm Zertifizierungsstelle ermitteln und dann ermitteln, ob Sie vertrauenswürdig ist.

Ebenso muss der Remote Host oder der lokale Computer bestimmen, ob das vom Benutzer oder der Anwendung vorgelegte Zertifikat authentisch ist. Das Zertifikat, das vom Benutzer über die LSA und SSPI vorgelegt wird, wird auf dem lokalen Computer für die lokale Anmeldung, im Netzwerk oder in der Domäne über die Zertifikat Speicher in Active Directory ausgewertet.

Um ein Zertifikat zu erhalten, werden die Authentifizierungsdaten durch Hash Algorithmen, wie z. b. Secure-Hash-Algorithmus 1 (SHA1), weitergeleitet, um einen Nachrichten Digest zu erhalten. Der Nachrichten Digest wird dann mithilfe des privaten Schlüssels des Absenders digital signiert, um nachzuweisen, dass der Nachrichten Digest vom Absender erstellt wurde.

NOTE

SHA1 ist die Standardeinstellung in Windows 7 und Windows Vista, wurde aber in Windows 8 in SHA2 geändert.

Smartcardauthentifizierung

Die Smartcard-Technologie ist ein Beispiel für eine Zertifikat basierte Authentifizierung. Die Anmeldung bei einem Netzwerk mit einer Smartcard bietet eine starke Form der Authentifizierung, da Sie eine kryptografiebasierte Identifikation und einen Nachweis des Besitzes verwendet, wenn ein Benutzer bei einer Domäne authentifiziert wird. Active Directory Zertifikat Dienste (AD CS) bieten die kryptografiebasierte Identifikation durch die Ausstellung eines Anmelde Zertifikats für jede Smartcard.

Informationen zur Smartcardauthentifizierung finden Sie in der [technischen Referenz für die Windows-Smartcard](#).

Die Technologie für virtuelle Smartcards wurde in Windows 8 eingeführt. Er speichert das Zertifikat der Smartcard auf dem PC und schützt es dann mithilfe des Sicherheitstokendienstes für den Geräte Manipulations Trusted Platform Module (TPM). Auf diese Weise wird der PC tatsächlich zur Smartcard, die die PIN des Benutzers erhalten muss, damit Sie authentifiziert werden kann.

Remote-und drahtlose Authentifizierung

Die Authentifizierung von Remote-und Drahtlos Netzwerken ist eine andere Technologie, die Zertifikate für die Authentifizierung verwendet. Der Internet Authentifizierungsdienst (IAS) und die virtuellen privaten Netzwerkserver verwenden das Extensible Authentication Protocol-Transport Level Security (EAP-TLS), PEAP (Protected Extensible Authentication Protocol) oder IPSec (Internet Protocol Security), um eine Zertifikat basierte Authentifizierung für viele Arten von Netzwerk Zugriff durchzuführen, einschließlich VPN (virtuelles privates

Netzwerk) und Drahtlos Verbindungen.

Informationen zur Zertifikat basierten Authentifizierung im Netzwerk finden Sie unter [Netzwerk Zugriffs Authentifizierung und-Zertifikate](#).

Siehe auch

[Windows-Authentifizierungskonzepte](#)

In der Windows-Authentifizierung verwendete Gruppenrichtlinieneinstellungen

09.04.2020 • 8 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Referenz Thema für IT-Experten werden die Verwendung und Auswirkung von Gruppenrichtlinie Einstellungen im Authentifizierungsprozess beschrieben.

Sie können die Authentifizierung in Windows-Betriebssystemen verwalten, indem Sie Benutzer-, Computer- und Dienst Konten zu Gruppen hinzufügen und anschließend Authentifizierungs Richtlinien für diese Gruppen anwenden. Diese Richtlinien werden als lokale Sicherheitsrichtlinien und als administrative Vorlagen definiert, auch als Gruppenrichtlinie Einstellungen bezeichnet. Beide Sätze können mit Gruppenrichtlinie in ihrer gesamten Organisation konfiguriert und verteilt werden.

NOTE

Mithilfe der in Windows Server 2012 R2 eingeführten Features können Sie Authentifizierungs Richtlinien für gezielte Dienste oder Anwendungen, die häufig als Authentifizierungs Silos bezeichnet werden, mithilfe geschützter Konten konfigurieren. Informationen dazu, wie Sie dies in Active Directory tun, finden Sie unter [Konfigurieren geschützter Konten](#).

Beispielsweise können Sie die folgenden Richtlinien auf Grundlage ihrer Funktion in der Organisation auf Gruppen anwenden:

- Lokal oder in einer Domäne anmelden
- Anmelden über ein Netzwerk
- Konten zurücksetzen
- Erstellen von Konten

In der folgenden Tabelle sind die für die-Authentifizierung relevanten Richtlinien Gruppen aufgeführt. es enthält Links zu Dokumentationen, mit denen Sie diese Richtlinien konfigurieren können.

| RICHTLINIEN GRUPPE | LOCATION | BESCHREIBUNG |
|----------------------|---|---|
| Kenn Wort Richtlinie | Lokaler Computer
policy\computerkonfiguration\windows-einstellungen\sicherheitseinstellungen\k
onto Richtlinien | Kenn Wort Richtlinien beeinflussen die Merkmale und das Verhalten von Kenn Wörtern. Kenn Wort Richtlinien werden für Domänen Konten oder lokale Benutzerkonten verwendet. Sie bestimmen Einstellungen für Kenn Wörter, z. b. Erzwingung und Lebensdauer.

Informationen zu bestimmten Einstellungen finden Sie unter Kenn Wort Richtlinie . |

| RICHTLINIEN GRUPPE | LOCATION | BESCHREIBUNG |
|------------------------|---|---|
| Konto Sperr Richtlinie | Lokaler Computer
policy\computerkonfiguration\windows-einstellungen\sicherheitseinstellungen\konto Richtlinien | <p>Optionen für die Konto Sperrungs Richtlinie deaktivieren Sie Konten nach einer festgelegten Anzahl fehlerhafter Anmeldeversuche. Mithilfe dieser Optionen können Sie Versuche zum Unterbrechen von Kenn Wörtern erkennen und blockieren.</p> <p>Informationen zu den Optionen für die Konto Sperrungs Richtlinie finden Sie unter Konto Sperr Richtlinie.</p> |
| Kerberos-Richtlinie | Lokaler Computer
policy\computerkonfiguration\windows-einstellungen\sicherheitseinstellungen\konto Richtlinien | <p>Die Kerberos-bezogenen Einstellungen umfassen die Ticket Lebensdauer und Erzwingungs Regeln. Die Kerberos-Richtlinie gilt nicht für lokale Konto Datenbanken, da das Kerberos-Authentifizierungsprotokoll nicht verwendet wird, um lokale Konten zu authentifizieren. Aus diesem Grund können die Kerberos-Richtlinien Einstellungen nur mithilfe des standardmäßigen Domänen Gruppenrichtlinie Objekts (GPO) konfiguriert werden, wo es sich auf Domänen Anmeldungen auswirkt.</p> <p>Informationen zu Kerberos-Richtlinien Optionen für den Domänen Controller finden Sie unter Kerberos-Richtlinie.</p> |
| Überwachungsrichtlinie | Lokaler Computer
policy\computerkonfiguration\windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien \ Überwachungsrichtlinie | <p>Mithilfe der Überwachungsrichtlinie können Sie den Zugriff auf Objekte, wie z. b. Dateien und Ordner, Steuern und verstehen sowie Benutzer-und Gruppenkonten sowie Benutzeranmeldungen und-Abrechnungen verwalten. Mit Überwachungs Richtlinien können die Kategorien von Ereignissen angegeben werden, die Sie überwachen möchten, die Größe und das Verhalten des Sicherheitsprotokolls festlegen und bestimmen, welche Objekte der Zugriff überwacht werden sollen und welche Art von Zugriff Sie überwachen möchten.</p> |

| RICHTLINIEN GRUPPE | LOCATION | BESCHREIBUNG |
|--------------------------------------|--|---|
| Zuweisung von Benutzerrechten | Lokale Computer
policy\computerkonfiguration\windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Zuweisen von Benutzerrechten | Benutzerrechte werden in der Regel auf Basis der Sicherheitsgruppen zugewiesen, zu denen ein Benutzer gehört, z. b. Administratoren, Hauptbenutzer oder Benutzer. Die Richtlinien Einstellungen in dieser Kategorie werden in der Regel verwendet, um Berechtigungen für den Zugriff auf einen Computer basierend auf der Zugriffs- und Sicherheitsgruppen Mitgliedschaften zu erteilen oder zu verweigern. |
| Sicherheitsoptionen | Lokale Computer
policy\computerkonfiguration\windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen | Zu den für die Authentifizierung relevanten Richtlinien gehören:
<ul style="list-style-type: none"> -Geräte -Domänen Controller -Domänen Mitglied -Interaktive Anmeldung -Microsoft-Netzwerkserver -Netzwerk Zugriff -Netzwerksicherheit -Wiederherstellungskonsole -Herunterfahren |
| Delegierungs Delegierungen | Computerkonfiguration\Administrative vorlagen\system\anmeldeinformationen Delegierung | Bei der Delegierung von Anmelde Informationen handelt es sich um einen Mechanismus, mit dem lokale Anmelde Informationen auf anderen Systemen verwendet werden können, insbesondere Mitglieds Server und Domänen Controller innerhalb einer Domäne. Diese Einstellungen gelten für Anwendungen mithilfe des Credential Security Support Provider (SSP). Remotedesktopverbindung ist ein Beispiel. |
| KDC | Computerkonfiguration\Administrative vorlagen\system\kdc | Diese Richtlinien Einstellungen wirken sich darauf aus, wie die Schlüsselverteilungscenter (KDC), bei der es sich um einen Dienst auf dem Domänen Controller handelt, Kerberos-Authentifizierungsanforderungen verarbeitet. |
| Kerberos | Computerkonfiguration\Administrative vorlagen\system\kerberos | Diese Richtlinien Einstellungen beeinflussen, wie Kerberos für die Unterstützung von Ansprüchen, Kerberos armoring, Verbund Authentifizierung, Identifizierung von Proxy Servern und anderen Konfigurationen konfiguriert ist. |
| Anmelden | Computerkonfiguration\Administrative Vorlagen\System\Anmeldung | Mit diesen Richtlinien Einstellungen wird gesteuert, wie das System den Anmeldevorgang für Benutzer anzeigt. |

| RICHTLINIEN GRUPPE | LOCATION | BESCHREIBUNG |
|--|---|---|
| Anmelde Namen | Computerkonfiguration\Administrative
vorlagen\system\net-Anmeldung | Mit diesen Richtlinien Einstellungen wird gesteuert, wie das System Netzwerk Anmelde Anforderungen behandelt, einschließlich der Art des Domänen Controller-Locators.

Weitere Informationen zur Funktionsweise des Domänen Controller-Locators in Replikations Prozesse finden Sie Untergrund Legendes zur Replikation Zwischenstand Orten . |
| Biometrie | Computerkonfiguration\Administrative
Vorlagen\Windows-
komponents\biometrie | Diese Richtlinien Einstellungen erlauben oder verweigern die Verwendung von Biometrie als Authentifizierungsmethode.

Weitere Informationen zur Windows-Implementierung von Biometrie finden Sie unter Windows-Biometrieframework Übersicht. |
| Anmelde Informationen-
Benutzeroberfläche | Computerkonfiguration\Administrative
Vorlagen\Windows-
komponents\benutzerbenutzerschnittst
elle | Diese Richtlinien Einstellungen steuern, wie Anmelde Informationen zum Zeitpunkt des Eintrags verwaltet werden. |
| Kenn Wort Synchronisierung | Computerkonfiguration\Administrative
Vorlagen\Windows-komponents\kenn
Wort Synchronisierung | Mit diesen Richtlinien Einstellungen wird festgelegt, wie das System die Synchronisierung von Kenn Wörtern zwischen Windows-und UNIX-basierten Betriebssystemen verwaltet.

Weitere Informationen finden Sie unter Kenn Wort Synchronisierung . |
| Smartcard | Computerkonfiguration\Administrative
Vorlagen\Windows-
komponents\smartcard | Mit diesen Richtlinien Einstellungen wird gesteuert, wie Smartcardanmeldungen vom System verwaltet werden. |
| Windows-Anmelde Optionen | Computerkonfiguration\Administrative
Vorlagen\Windows-
komponents\windows-Anmelde
Optionen | Diese Richtlinien Einstellungen steuern, wann und wie Anmelde Chancen verfügbar sind. |
| STRG + ALT + ENTF-Optionen | Computerkonfiguration\Administrative
Vorlagen\Windows-komponents\strg +
ALT + ENTF-Optionen | Diese Richtlinien Einstellungen wirken sich auf die Darstellung von und den Zugriff auf Funktionen auf der Anmelde Benutzeroberfläche (sicherer Desktop) aus, z. b. Task-Manager und die Tastatursperre des Computers. |
| Anmelden | Computerkonfiguration\Administrative
Vorlagen\Windows-komponents\logon | Mit diesen Richtlinien Einstellungen wird festgelegt, ob oder welche Prozesse ausgeführt werden können, wenn sich der Benutzer anmeldet. |

Siehe auch

[Windows-Authentifizierung: Technische Übersicht](#)

Schutz und Verwaltung von Anmeldeinformationen

09.04.2020 • 7 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema für IT-Experten werden die in Windows Server 2012 R2 eingeführten Features und Methoden sowie die Windows 8.1 für den Schutz von Anmelde Informationen und die Domänen Authentifizierung erläutert, um den Diebstahl von Anmelde Informationen zu verringern.

Eingeschränkter Administratormodus für die Remotedesktopverbindung

Der eingeschränkte Administratormodus stellt eine Methode zum interaktiven Protokollieren auf einem Remotehostserver dar, bei dem Ihre Anmeldeinformationen nicht an den Server übermittelt werden. Dadurch wird verhindert, dass Ihre Anmeldeinformationen beim anfänglichen Verbindungsprozess abgefangen werden, wenn der Server gefährdet ist.

Durch die Verwendung dieses Modus mit Administratoranmeldeinformationen versucht der Remotedesktopclient, sich interaktiv auf einem Host anzumelden, der diesen Modus ebenfalls unterstützt, ohne Anmeldeinformationen zu senden. Die Verbindung wird erfolgreich hergestellt, wenn der Host bestätigt hat, dass das Benutzerkonto, das die Verbindung herstellt, über Administratorrechte verfügt und den eingeschränkten Administratormodus unterstützt. Andernfalls schlägt der Verbindungsversuch fehl. Beim eingeschränkten Administratormodus werden Anmeldeinformationen nie als Nur-Text oder in einer anderen wiederverwendbaren Form an Remotecomputer gesendet.

LSA-Schutz

Mithilfe der lokalen Sicherheitsautorität (Local Security Authority, LSA), die sich im LSASS-Prozess (Local Security Authority Security Service, Sicherheitsdienst für die lokale Sicherheitsautorität) befindet, werden Benutzer für die lokale Anmeldung und Remoteanmeldung überprüft und lokale Sicherheitsrichtlinien erzwungen. Das Betriebssystem Windows 8.1 bietet zusätzlichen Schutz für die LSA, um die Code Injektion durch nicht geschützte Prozesse zu verhindern. Dies sorgt für eine erhöhte Sicherheit in Bezug auf Anmeldeinformationen, die von der lokalen Sicherheitsautorität gespeichert und verwaltet werden. Diese geschützte Prozess Einstellung für LSA kann in Windows 8.1 konfiguriert werden, ist in Windows RT 8,1 jedoch standardmäßig aktiviert und kann nicht geändert werden.

Weitere Informationen zum Konfigurieren des LSA-Schutzes finden Sie unter [Configuring Additional LSA Protection](#).

Sicherheitsgruppe "Geschützte Benutzer"

Diese neue globale Gruppe der Domäne löst neuen, nicht konfigurierbaren Schutz auf Geräten und Host Computern aus, auf denen Windows Server 2012 R2 und Windows 8.1 ausgeführt wird. Die Gruppe "geschützte Benutzer" ermöglicht zusätzlichen Schutz für Domänen Controller und Domänen in Windows Server 2012 R2-Domänen. Dadurch werden die Anmeldeinformationstypen erheblich verringert, die verfügbar sind, wenn Benutzer über einen nicht gefährdeten Computer auf Computern im Netzwerk angemeldet sind.

Mitglieder der Gruppe "Geschützte Benutzer" werden mithilfe der folgenden Authentifizierungsmethoden weiter eingeschränkt:

- Ein Mitglied der Gruppe "Geschützte Benutzer" kann sich nur über das Kerberos-Protokoll anmelden. Das Konto kann nicht mithilfe von NTLM, Digestauthentifizierung oder CredSSP authentifiziert werden. Auf einem Gerät, auf dem Windows 8.1 ausgeführt wird, werden Kenn Wörter nicht zwischengespeichert, sodass das Gerät, das einen dieser SSPs (Security Support Providers) verwendet, nicht bei einer Domäne

authentifiziert werden kann, wenn das Konto Mitglied der Gruppe der geschützten Benutzer ist.

- Das Kerberos-Protokoll verwendet die schwächeren Verschlüsselungstypen DES oder RC4 nicht im Vorauthentifizierungsprozess. Daher muss die Domäne so konfiguriert werden, dass mindestens die Verschlüsselungssammlung AES unterstützt wird.
- Das Konto des Benutzers kann nicht mit eingeschränkter oder nicht eingeschränkter Kerberos-Delegierung delegiert werden. Das bedeutet, dass frühere Verbindungen mit anderen Systemen fehlschlagen, wenn der Benutzer Mitglied der Gruppe "Geschützte Benutzer" ist.
- Die Standardeinstellung für die Lebensdauer von Kerberos-TGTs (Ticket Granting Tickets) von vier Stunden kann mit Authentifizierungsrichtlinien und -silos konfiguriert werden, auf die über das Active Directory-Verwaltungscenter zugegriffen werden kann. Das heißt, dass sich der Benutzer nach Ablauf von vier Stunden erneut authentifizieren muss.

WARNING

Konten für Dienste und Computer sollten nicht Mitglieder der Benutzergruppe Geschützte Benutzer sein. Diese Gruppe bietet keinen lokalen Schutz, da das Kennwort oder Zertifikat immer auf dem Host verfügbar ist. Die Authentifizierung schlägt mit dem Fehler "der Benutzername oder das Kennwort ist falsch" für jeden Dienst oder Computer fehl, der der Gruppe "geschützte Benutzer" hinzugefügt wird.

Weitere Informationen zu dieser Gruppe finden Sie unter [Sicherheitsgruppe "Geschützte Benutzer"](#).

Authentifizierungsrichtlinie und Authentifizierungsrichtliniensilos

Gesamtstruktur basierte Active Directory Richtlinien werden eingeführt und können auf Konten in einer Domäne mit einer Windows Server 2012 R2-Domänen Funktionsebene angewendet werden. Mit diesen Authentifizierungsrichtlinien kann gesteuert werden, welche Hosts ein Benutzer zum Anmelden verwenden kann. Sie werden in Verbindung mit der Sicherheitsgruppe „Geschützte Benutzer“ verwendet, und Administratoren können auf die Konten Zugriffssteuerungsbedingungen zur Authentifizierung anwenden. Diese Authentifizierungsrichtlinien isolieren zugehörige Konten, um den Gültigkeitsbereich eines Netzwerks zu beschränken.

Mit der neuen Active Directory Objektklasse "Authentifizierungs Richtlinie" können Sie die Authentifizierungs Konfiguration auf Konto Klassen in Domänen mit einer Windows Server 2012 R2-Domänen Funktionsebene anwenden. Authentifizierungsrichtlinien werden während des Austauschs des Authentifizierungsdiensts (Authentication Service, AS) und des Ticket-Granting Service (TGS) des Kerberos-Protokolls erzwungen. Es existieren die folgenden Active Directory-Kontoklassen:

- Benutzer
- Computer
- Verwaltetes Dienstkonto
- Gruppenverwaltetes Dienstkonto

Weitere Informationen finden Sie unter [Authentifizierungsrichtlinien und Authentifizierungsrichtliniensilos](#).

Weitere Informationen zum Konfigurieren geschützter Konten finden Sie unter [Konfigurieren geschützter Konten](#).

Siehe auch

Weitere Informationen zu LSA und LSASS finden Sie unter [Technische Übersicht über die Windows-Anmeldung und -Authentifizierung](#).

Konfigurieren von zusätzlichem LSA-Schutz

09.04.2020 • 17 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema für IT-Spezialisten erfahren Sie, wie Sie den zusätzlichen Schutz für den Prozess der lokalen Sicherheitsautorität (Local Security Authority, LSA) konfigurieren, um eine Codeinjizierung mit einer möglichen Beeinträchtigung der Anmeldeinformationen zu verhindern.

Mithilfe der lokalen Sicherheitsautorität, die auch den LSASS-Prozess (Local Security Authority Subsystem Service, Subsystemdienst für die lokale Sicherheitsautorität) umfasst, werden Benutzer für die lokale Anmeldung und Remoteanmeldung überprüft und lokale Sicherheitsrichtlinien erzwungen. Das Betriebssystem Windows 8.1 bietet zusätzlichen Schutz für die LSA, um das Lesen von Speicher und Code Injektion durch nicht geschützte Prozesse zu verhindern. Dies sorgt für eine erhöhte Sicherheit in Bezug auf Anmeldeinformationen, die von der lokalen Sicherheitsautorität gespeichert und verwaltet werden. Die geschützte Prozess Einstellung für LSA kann in Windows 8.1 konfiguriert werden, Sie kann jedoch nicht in Windows RT 8,1 konfiguriert werden. Wenn diese Einstellung zusammen mit dem sicheren Start verwendet wird, erhöht dies den Schutz, da das Deaktivieren des Registrierungsschlüssels HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa keine Wirkung hat.

Anforderungen an den geschützten Prozess für Plug-Ins oder Treiber

Damit ein LSA-Plug-In oder -Treiber erfolgreich als geschützter Prozess geladen werden kann, muss er die folgenden Kriterien erfüllen:

1. Signaturüberprüfung

Der geschützte Modus erfordert, dass alle Plug-Ins, die in die lokale Sicherheitsautorität geladen werden, mit einer Microsoft-Signatur digital signiert werden. Daher können alle Plug-Ins, die nicht signiert sind bzw. nicht mit einer Microsoft-Signatur signiert sind, in der lokalen Sicherheitsautorität nicht geladen werden. Beispiele für diese Plug-Ins sind Smartcard-Treiber, kryptografische Plug-Ins und Kennwortfilter.

LSA-Plug-Ins, bei denen es sich um Treiber handelt, z. B. Smartcard-Treiber, müssen mithilfe der WHQL-Zertifizierung signiert werden. Weitere Informationen finden Sie unter [WHQL-releasesignatur](#).

LSA-Plug-Ins, die nicht über einen WHQL-Zertifizierungsprozess verfügen, müssen mithilfe des [Dateisignierdiensts für LSA](#) signiert werden.

2. Anleitung zur Einhaltung des Microsoft Security Development Lifecycle (SDL)-Prozesses

Alle Plug-Ins müssen die Vorgaben zur Einhaltung des jeweiligen SDL-Prozesses erfüllen. Weitere Informationen finden Sie unter [Microsoft Security Development Lifecycle \(SDL\) – Anhang](#).

Auch wenn die Plug-Ins ordnungsgemäß mit einer Microsoft-Signatur signiert sind, kann eine Nichteinhaltung des SDL-Prozesses beim Laden eines Plug-Ins zu einem Fehler führen.

Empfohlene Vorgehensweisen

Nutzen Sie die folgende Liste, um eingehend zu testen, ob der LSA-Schutz aktiviert ist, bevor Sie das Feature allgemein bereitstellen:

- Identifizieren Sie alle LSA-Plug-Ins und -Treiber, die in Ihrer Organisation verwendet werden. Dazu gehören nicht von Microsoft stammende Treiber oder Plug-Ins, z. B. Smartcard-Treiber und kryptografische Plug-Ins, und eine intern entwickelte Software, die eingesetzt wird, um Kennwortfilter oder Benachrichtigungen über Kennwortänderungen zu erzwingen.

- Stellen Sie sicher, dass alle LSA-Plug-Ins digital mit einem Microsoft-Zertifikat signiert sind, damit beim Laden des Plug-Ins kein Fehler auftritt.
- Stellen Sie sicher, dass alle ordnungsgemäß signierten Plug-Ins erfolgreich in die lokale Sicherheitsautorität geladen werden können und dass sie sich wie erwartet verhalten.
- Verwenden Sie die Überwachungsprotokolle zum Identifizieren von LSA-Plug-Ins und -Treibern, die nicht als geschützter Prozess ausgeführt werden können.

Mit aktiviertem LSA-Schutz eingeführte Einschränkungen

Wenn LSA-Schutz aktiviert ist, können Sie kein benutzerdefiniertes LSA-Plug-in Debuggen. Es ist nicht möglich, einen Debugger an LSASS anzufügen, wenn es sich um einen geschützten Prozess handelt. Im Allgemeinen gibt es keine unterstützte Möglichkeit zum Debuggen eines laufenden geschützten Prozesses.

Identifizieren von LSA-Plug-Ins und -Treibern, die nicht als geschützter Prozess ausgeführt werden können

Die in diesem Abschnitt beschriebenen Ereignisse sind im Betriebsprotokoll unter `%%"Anwendungs- und Dienstprotokolle\Microsoft\Windows\CodeIntegrity%%"` enthalten. Sie stellen eine Hilfe beim Identifizieren von LSA-Plug-Ins und -Treibern dar, die aufgrund von Signaturproblemen nicht geladen werden können. Zum Verwalten dieser Ereignisse können Sie das Befehlszeilentool **wevtutil** verwenden. Informationen zu diesem Befehl finden Sie unter [Wevtutil](#).

Vor der Aktivierung: Identifizieren von Plug-Ins und Treibern, die von "lsass.exe" geladen werden

Mithilfe des Überwachungsmodus können Sie LSA-Plug-Ins und -Treiber identifizieren, die im LSA-Schutzmodus nicht geladen werden können. Im Überwachungsmodus werden vom System Ereignisprotokolle generiert und alle Plug-Ins und Treiber identifiziert, die unter der lokalen Sicherheitsautorität nicht geladen werden können, wenn der LSA-Schutz aktiviert ist. Die Meldungen werden protokolliert, ohne die Plug-Ins oder Treiber zu blockieren.

So aktivieren Sie den Überwachungsmodus für `%%"lsass.exe%%"` auf einem einzelnen Computer per Bearbeitung der Registrierung

1. Öffnen Sie den Registrierungs-Editor (RegEdit.exe), und navigieren Sie zum Registrierungsschlüssel unter `%%"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LSASS.exe%%"`.
2. Legen Sie den Wert des Registrierungsschlüssels wie folgt fest: **AuditLevel=dword:00000008**.
3. Starten Sie den Computer neu.

Analysieren Sie die Ergebnisse von Ereignis 3065 und Ereignis 3066.

Anschließend werden diese Ereignisse möglicherweise in Ereignisanzeige angezeigt: Microsoft-Windows-codeintegrity/Operational:

- **Ereignis 3065:** Mit diesem Ereignis wird aufgezeichnet, dass bei einer Codeintegritätsprüfung ermittelt wurde, dass ein Prozess (normalerweise `%%"lsass.exe%%"`) einen bestimmten Treiber zu laden versucht hat, der die Sicherheitsanforderungen für freigegebene Abschnitte nicht erfüllt. Aufgrund der festgelegten Systemrichtlinie wurde das Laden des Images jedoch zugelassen.
- **Ereignis 3066:** Mit diesem Ereignis wird aufgezeichnet, dass bei einer Codeintegritätsprüfung ermittelt wurde, dass ein Prozess (normalerweise `%%"lsass.exe%%"`) einen bestimmten Treiber zu laden versucht hat, der die Anforderungen an die Microsoft-Signatureebene nicht erfüllt. Aufgrund der festgelegten Systemrichtlinie wurde das Laden des Images jedoch zugelassen.

IMPORTANT

Diese Betriebsereignisse werden nicht generiert, wenn auf einem System ein Kerneldebugger angefügt und aktiviert ist.

Wenn ein Plug-In oder Treiber freigegebene Abschnitte enthält, wird Ereignis 3066 zusammen mit dem Ereignis 3065 protokolliert. Durch das Entfernen der freigegebenen Abschnitte sollte verhindert werden, dass diese beiden Ereignisse eintreten, es sei denn, das Plug-In erfüllt die Anforderungen an die Microsoft-Signatureebene nicht.

Zum Aktivieren des Überwachungsmodus für mehrere Computer in einer Domäne können Sie die clientseitige Registrierungserweiterung für die Gruppenrichtlinie verwenden, um den Überwachungsebenen-Registrierungswert für `\"Lsass.exe\"` bereitzustellen. Sie müssen den Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LSASS.exe\"` ändern.

So erstellen Sie die Einstellung des AuditLevel-Werts in einem Gruppenrichtlinienobjekt

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsolle (GPMC).
2. Erstellen Sie ein neues Gruppenrichtlinienobjekt (Group Policy Object, GPO), das auf der Domänenebene verknüpft ist oder das mit der Organisationseinheit verknüpft ist, die Ihre Computerkonten enthält. Alternativ dazu können Sie ein GPO auswählen, das schon bereitgestellt wurde.
3. Klicken Sie mit der rechten Maustaste auf das Gruppenrichtlinienobjekt, und klicken Sie dann auf **Bearbeiten**, um den Gruppenrichtlinienverwaltungs-Editor zu öffnen.
4. Erweitern Sie nacheinander **Computerkonfiguration**, **Einstellungen** und dann **Windows-Einstellungen**.
5. Klicken Sie mit der rechten Maustaste auf **Registrierung**, zeigen Sie auf **Neu**, und klicken Sie dann auf **Registrierungselement**. Das Dialogfeld **Neue Registrierungseigenschaften** wird angezeigt.
6. Klicken Sie in der Liste **Struktur** auf **HKEY_LOCAL_MACHINE**.
7. Navigieren Sie in der Liste **Schlüsselpfad** zu **SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LSASS.exe**.
8. Geben Sie im Feld **Wertname** Folgendes ein: **AuditLevel**.
9. Klicken Sie im Feld **Werttyp** auf **REG_DWORD**, um diese Option auszuwählen.
10. Geben Sie im Feld **Wert** Folgendes ein: **00000008**.
11. Klicken Sie auf **OK**.

NOTE

Damit das GPO wirksam wird, muss die GPO-Änderung auf alle Domänencontroller der Domäne repliziert werden.

Zum Aktivieren des zusätzlichen LSA-Schutzes auf mehreren Computern können Sie die clientseitige Registrierungserweiterung für die Gruppenrichtlinie verwenden, indem Sie `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\"` ändern. Informationen zu den erforderlichen Schritten finden Sie unter [Konfigurieren des zusätzlichen LSA-Schutzes für Anmeldeinformationen](#) in diesem Thema.

Nach der Aktivierung: Identifizieren von Plug-Ins und Treibern, die von "Lsass.exe" geladen werden

Sie können das Ereignisprotokoll verwenden, um LSA-Plug-Ins und -Treiber zu identifizieren, die im LSA-Schutzmodus nicht geladen werden konnten. Wenn der per LSA geschützte Prozess aktiviert ist, werden vom System Ereignisprotokolle generiert. Damit können alle Plug-Ins und Treiber identifiziert werden, die im LSA-

Modus nicht geladen werden konnten.

Analysieren Sie die Ergebnisse von Ereignis 3033 und Ereignis 3063.

Anschließend werden diese Ereignisse möglicherweise in Ereignisanzeige angezeigt: Microsoft-Windows-codeintegrity/Operational:

- **Ereignis 3033:** Mit diesem Ereignis wird aufgezeichnet, dass bei einer Codeintegritätsprüfung ermittelt wurde, dass ein Prozess (normalerweise `lsass.exe`) einen Treiber zu laden versucht hat, der die Anforderungen an die Microsoft-Signatureebene nicht erfüllt.
- **Ereignis 3063:** Mit diesem Ereignis wird aufgezeichnet, dass bei einer Codeintegritätsprüfung ermittelt wurde, dass ein Prozess (normalerweise `lsass.exe`) einen Treiber zu laden versucht hat, der die Sicherheitsanforderungen für freigegebene Abschnitte nicht erfüllt.

Freigegebene Abschnitte sind in der Regel das Ergebnis von Programmier Techniken, bei denen Instanzdaten mit anderen Prozessen interagieren können, für die der gleiche Sicherheitskontext verwendet wird. Dies kann zu Sicherheitsrisiken führen.

Konfigurieren des zusätzlichen LSA-Schutzes für Anmeldeinformationen

Auf Geräten mit Windows 8.1 (mit oder ohne sicheren Start oder UEFI) ist die Konfiguration möglich, indem die in diesem Abschnitt beschriebenen Verfahren ausgeführt werden. Bei Geräten, auf denen Windows RT 8,1 ausgeführt wird, ist der Schutz von LSASS.exe immer aktiviert und kann nicht deaktiviert werden.

Auf x86-basierten oder x64-basierten Geräten mit oder ohne `Sicherer Start` und UEFI

Auf x86- oder x64-basierten Geräten, von denen der sichere Start oder UEFI verwendet wird, wird in der UEFI-Firmware eine UEFI-Variable festgelegt, wenn der LSA-Schutz mithilfe des Registrierungsschlüssels aktiviert wird. Wenn die Einstellung in der Firmware gespeichert wird, kann die UEFI-Variable im Registrierungsschlüssel nicht gelöscht oder geändert werden. Die UEFI-Variable muss zurückgesetzt werden.

x86-basierte oder x64-basierte Geräte, die UEFI oder `Sicherer Start` nicht unterstützen, werden deaktiviert, können die Konfiguration für den LSA-Schutz in der Firmware nicht speichern und sind vollständig vom Vorhandensein des Registrierungsschlüssels abhängig. In diesem Fall ist es möglich, den LSA-Schutz zu deaktivieren, indem der Remotezugriff auf das Gerät genutzt wird.

Sie können die folgenden Verfahren verwenden, um den LSA-Schutz zu aktivieren oder zu deaktivieren:

So aktivieren Sie den LSA-Schutz auf einem einzelnen Computer

1. Öffnen Sie den Registrierungs-Editor (RegEdit.exe), und navigieren Sie zum Registrierungsschlüssel unter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`.
2. Legen Sie den Wert des Registrierungsschlüssels wie folgt fest: "RunAsPPL"=dword:00000001.
3. Starten Sie den Computer neu.

So aktivieren Sie den LSA-Schutz mithilfe der Gruppenrichtlinie

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskontrolle (GPMC).
2. Erstellen Sie ein neues Gruppenrichtlinienobjekt, das auf der Domänenebene verknüpft ist oder das mit der Organisationseinheit verknüpft ist, die Ihre Computerkonten enthält. Alternativ dazu können Sie ein GPO auswählen, das schon bereitgestellt wurde.
3. Klicken Sie mit der rechten Maustaste auf das Gruppenrichtlinienobjekt, und klicken Sie dann auf **Bearbeiten**, um den Gruppenrichtlinienverwaltungs-Editor zu öffnen.
4. Erweitern Sie nacheinander **Computerkonfiguration**, **Einstellungen** und dann **Windows-**

Einstellungen.

5. Klicken Sie mit der rechten Maustaste auf **Registrierung**, zeigen Sie auf **Neu**, und klicken Sie dann auf **Registrierungselement**. Das Dialogfeld **Neue Registrierungseigenschaften** wird angezeigt.
6. Klicken Sie in der Liste **Struktur** auf **HKEY_LOCAL_MACHINE**.
7. Navigieren Sie in der Liste **Schlüsselpfad** zu **SYSTEM\CurrentControlSet\Control\Lsa**.
8. Geben Sie im Feld **Wertname** Folgendes ein: **RunAsPPL**.
9. Klicken Sie im Feld **Werttyp** auf **REG_DWORD**.
10. Geben Sie im Feld **Wert** Folgendes ein: **00000001**.
11. Klicken Sie auf **OK**.

So deaktivieren Sie den LSA-Schutz

1. Öffnen Sie den Registrierungs-Editor (RegEdit.exe), und navigieren Sie zum Registrierungsschlüssel unter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`.
2. Löschen Sie den folgenden Wert aus dem Registrierungsschlüssel: "RunAsPPL"=dword:00000001.
3. Verwenden Sie das Tool zum Deaktivieren des geschützten LSA-Prozesses (Local Security Authority (LSA) Protected Process Opt-out), um die UEFI-Variable zu löschen, wenn für das Gerät "Sicherer Start" genutzt wird.

Weitere Informationen zu diesem Tool finden Sie auf der [Seite zum Download von Local Security Authority \(LSA\) Protected Process Opt-out im offiziellen Microsoft Download Center](#).

Weitere Informationen zum Verwalten von "Sicherer Start" finden Sie unter [UEFI-Firmware](#).

WARNING

Wenn "Sicherer Start" deaktiviert ist, werden alle auf "Sicherer Start" und UEFI bezogenen Konfigurationen zurückgesetzt. Sie sollten "Sicherer Start" nur deaktivieren, wenn alle anderen Mittel zum Deaktivieren des LSA-Schutzes nicht zum Erfolg führen.

Überprüfen des LSA-Schutzes

Wenn Sie ermitteln möchten, ob LSA beim Starten von Windows im geschützten Modus gestartet wurde, können Sie im Protokoll **System** unter **Windows-Protokolle** nach dem folgenden WinInit-Ereignis suchen:

- 12: LSASS.exe wurde als geschützter Prozess mit folgender Stufe gestartet: 4

Weitere Ressourcen

[Schutz und Verwaltung von Anmeldeinformationen](#)

[Datei Signatur Dienst für LSA](#)

Neues beim Schutz von Anmelde Informationen

09.04.2020 • 5 minutes to read • [Edit Online](#)

Credential Guard für angemeldeten Benutzer

Ab Windows 10, Version 1507, Kerberos und NTLM, verwenden Sie virtualisierungsbasierte Sicherheit, um Kerberos- & NTLM-Geheimnisse der Anmelde Sitzung des angemeldeten Benutzers zu schützen.

Ab Windows 10, Version 1511, verwendet Anmelde Informationen Manager die virtualisierungsbasierte Sicherheit, um gespeicherte Anmelde Informationen des Domänen Anmelde Informations Typs zu schützen. Anmelde Informationen und gespeicherte Domänen Anmelde Informationen werden nicht mithilfe von Remote Desktop an einen Remote Host übermittelt. Credential Guard kann ohne UEFI-Sperre aktiviert werden.

Ab Windows 10, Version 1607, ist der isolierte Benutzermodus in Hyper-V enthalten, sodass er nicht mehr separat für die Credential Guard-Bereitstellung installiert wird.

[Erfahren Sie mehr über Credential Guard.](#)

Remote Credential Guard für angemeldeten Benutzer

Ab Windows 10, Version 1607, schützt Remote Credential Guard Anmelde Informationen für angemeldete Benutzer, wenn Remotedesktop, indem die Kerberos- und NTLM-Geheimnisse auf dem Client Gerät geschützt werden. Damit der Remote Host die Netzwerkressourcen als Benutzer bewerten kann, müssen die geheimen Anforderungen vom Client Gerät verwendet werden.

Ab Windows 10, Version 1703, schützt Remote Credential Guard bereitgestellte Benutzer Anmelde Informationen, wenn Sie Remotedesktop verwenden.

[Erfahren Sie mehr über Remote Anmelde Informationen Guard.](#)

Domänen Schutz

Für den Domänen Schutz ist eine Active Directory Domäne erforderlich.

Unterstützung von in die Domäne eingebundenen Geräten für die Authentifizierung mit öffentlichem Schlüssel

Ab Windows 10, Version 1507 und Windows Server 2016, kann das Gerät mithilfe der Kerberos PKINIT-Authentifizierung bei einem Windows Server 2016-Domänen Controller mit dem öffentlichen Schlüssel authentifiziert werden, wenn ein in eine Domäne eingebundenes Gerät seinen gebundenen öffentlichen Schlüssel bei einem Windows Server 2016-Domänen Controller (DC) registrieren kann.

Ab Windows Server 2016 unterstützen KDCs die Authentifizierung mithilfe der Kerberos-Schlüssel Vertrauensstellung.

[Erfahren Sie mehr über die Unterstützung öffentlicher Schlüssel für in die Domäne eingebundenen Geräten & Kerberos-Schlüssel Vertrauen.](#)

PKINIT-Aktualität-Erweiterungs Unterstützung

Ab Windows 10, Version 1507 und Windows Server 2016, versuchen die Kerberos-Clients, die PKINIT-Aktualitäts Erweiterung für Anmeldungen mit öffentlichem Schlüssel zu unterstützen.

Ab Windows Server 2016 können KDCs die Erweiterung PKINIT-Aktualität unterstützen. Standardmäßig bieten KDCs keine PKINIT-Aktualität-Erweiterung.

Nur die NTLM-Geheimnisse des öffentlichen Schlüssels des öffentlichen Schlüssels

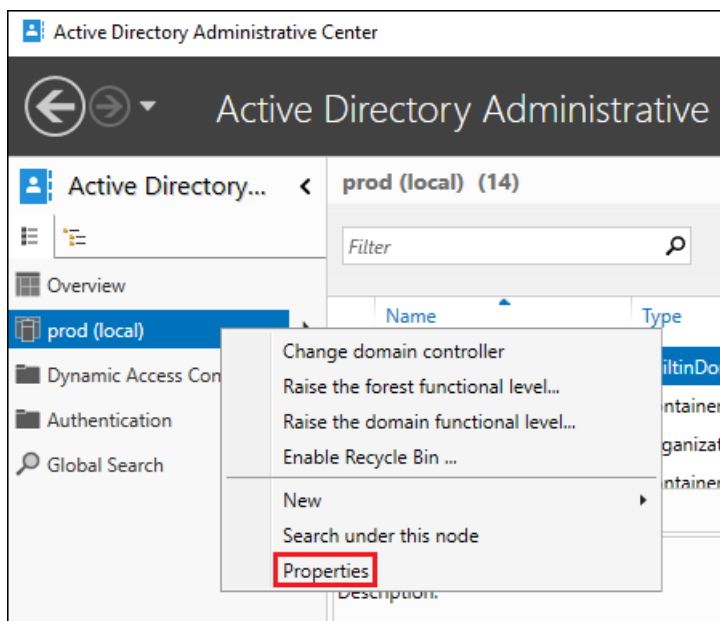
Beginnend mit der Windows Server 2016-Domänen Funktionsebene (DFL) können DCS die NTLM-Geheimnisse eines öffentlichen Schlüssels eines öffentlichen Schlüssels unterstützen. Diese Funktion ist in niedrigeren dfls nicht verfügbar.

WARNING

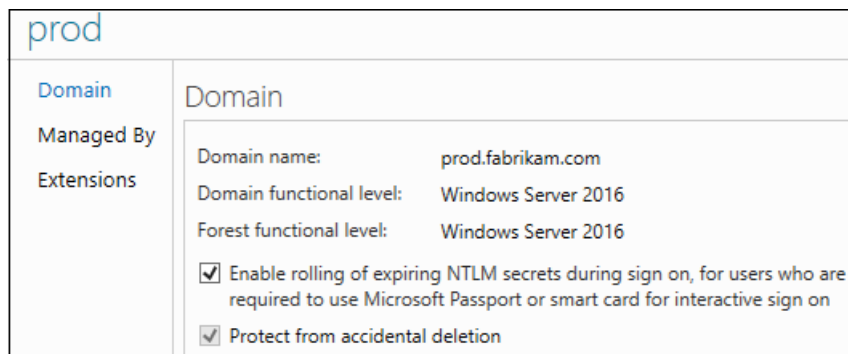
Wenn Sie einen Domänen Controller zu einer Domäne hinzufügen, bei der parallele NTLM-Geheimnisse aktiviert sind 2016, bevor der DC mit mindestens dem 8

Konfiguration: für neue Domänen ist dieses Feature standardmäßig aktiviert. Für vorhandene Domänen muss Sie im Active Directory Verwaltungs Center konfiguriert werden:

1. Klicken Sie im Active Directory Verwaltungs Center im linken Bereich mit der rechten Maustaste auf die Domäne, und wählen Sie **Eigenschaften** aus.



2. Aktivieren Sie das **Aktivieren des Rollbacks abgelaufener NTLM-Geheimnisse während der Anmeldung**, für Benutzer, die Microsoft Passport oder Smartcard für die interaktive Anmeldung verwenden müssen.



3. Klicken Sie auf **OK**.

Netzwerk-NTLM zulassen, wenn der Benutzer auf bestimmte in die Domäne eingebundenen Geräte beschränkt ist

Beginnend mit der Windows Server 2016-Domänen Funktionsebene (DFL) können DCS das Zulassen von Netzwerk-NTLM unterstützen, wenn ein Benutzer auf bestimmte in die Domäne eingebundenen Geräte beschränkt

ist. Diese Funktion ist in niedrigeren dfls nicht verfügbar.

Konfiguration: Klicken Sie in der Authentifizierungs Richtlinie auf **NTLM-Netzwerk Authentifizierung zulassen, wenn der Benutzer auf ausgewählte Geräte beschränkt ist**.

[Weitere Informationen zu Authentifizierungs Richtlinien.](#)

Sicherheitsgruppe „Geschützte Benutzer“

09.04.2020 • 11 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Thema für IT-Experten beschreibt die Active Directory-Sicherheitsgruppe „Geschützte Benutzer“ und erklärt deren Funktionsweise. Diese Gruppe wurde in Windows Server 2012 R2-Domänen Controllern eingeführt.

Übersicht über

Diese Sicherheitsgruppe ist als Teil einer Strategie zum Verwalten der Gefährdung von Anmelde Informationen innerhalb des Unternehmens konzipiert. Für Mitglieder dieser Gruppe gilt automatisch nicht konfigurierbarer Schutz für deren Konten. Eine Mitgliedschaft in der Gruppe der geschützten Benutzer bedeutet standardmäßig eine restriktive und proaktive Sicherheit. Die einzige Methode zum Ändern dieses Schutzes für ein Konto ist die Entfernung dieses Kontos aus der Sicherheitsgruppe.

WARNING

Konten für Dienste und Computer sollten nie Mitglied der Gruppe "geschützte Benutzer" sein. Diese Gruppe bietet trotzdem unvollständigen Schutz, da das Kennwort oder Zertifikat immer auf dem Host verfügbar ist. Bei der Authentifizierung tritt ein Fehler auf, "der Benutzername oder das Kennwort für alle Dienste oder Computer, die der Gruppe der geschützten Benutzer hinzugefügt wurden, nicht korrekt".

Diese Domänen bezogene globale Gruppe löst nicht konfigurierbaren Schutz auf Geräten und Host Computern aus, auf denen Windows Server 2012 R2 ausgeführt wird, und Windows 8.1 oder höher für Benutzer in Domänen mit einem primären Domänen Controller, auf dem Windows Server 2012 R2 ausgeführt wird. Dadurch wird der Standard Speicherbedarf von Anmelde Informationen erheblich reduziert, wenn Benutzer sich mit diesen Schutzvorrichtungen bei Computern anmelden.

Weitere Informationen finden Sie unter [Funktionsweise der Gruppe "geschützte Benutzer"](#) in diesem Thema.

Anforderungen der Gruppe "geschützte Benutzer"

Zum Bereitstellen von Geräteschutz für Mitglieder der Gruppe "geschützte Benutzer" müssen folgende Anforderungen erfüllt sein:

- Die globale Sicherheitsgruppe der geschützten Benutzer wird zu allen Domänencontrollern in der Kontodomäne repliziert.
- Windows 8.1 und Windows Server 2012 R2 haben standardmäßig Unterstützung hinzugefügt. Die [Microsoft-Sicherheitsempfehlung 2871997](#) bietet Unterstützung für Windows 7, Windows Server 2008 R2 und Windows Server 2012.

Folgende Anforderungen müssen erfüllt sein, damit Mitglieder der Gruppe der geschützten Benutzer Domänencontrollerschutz erhalten:

- Benutzer müssen sich in Domänen befinden, die die Domänen Funktionsebene Windows Server 2012 R2 oder höher aufweisen.

Hinzufügen geschützter Benutzer globaler Sicherheitsgruppen zu untergeordneten Domänen

Domänen Controller, auf denen ein älteres Betriebssystem als Windows Server 2012 R2 ausgeführt wird, können

das Hinzufügen von Mitgliedern zur neuen Sicherheitsgruppe für geschützte Benutzer unterstützen. Dies ermöglicht es den Benutzern, vor dem Upgrade der Domäne vom Geräteschutz zu profitieren.

NOTE

Domänen Controller werden von den Domänen Controllern nicht unterstützt.

Die Gruppe "geschützte Benutzer" kann erstellt werden, indem die Rolle "primärer Domänen Controller (PDC)" auf einen Domänen Controller mit Windows Server 2012 R2 übertragen wird. Nachdem das Gruppenobjekt auf andere Domänencontroller repliziert wurde, kann die PDC-Emulatorrolle auf einem Domänencontroller gehostet werden, der unter einer älteren Windows Server-Version läuft.

Eigenschaften der Gruppe "geschützte Benutzer"

Die folgende Tabelle zeigt die Eigenschaften der Gruppe der geschützten Benutzer.

| ATTRIBUT | WERT |
|--|-------------------------------|
| Gut bekannte SID/RID | S-1-5-21--525 |
| Typ | Globale Domäne |
| Standardcontainer | CN=Benutzer, DC=, DC= |
| Standardmitglieder | Keine |
| Standardmitglied von | Keine |
| Geschützt durch ADMINSDHOLDER? | Nein |
| Speichern, um aus Standardcontainer zu entfernen? | Ja |
| Speichern, um die Verwaltung dieser Gruppe zu Nicht-Dienstadministratoren zu delegieren? | Nein |
| Standardbenutzerrechte | Keine Standardbenutzerrechte. |

Funktionsweise der Gruppe "geschützte Benutzer"

In diesem Abschnitt wird erklärt, wie die Gruppe der geschützten Benutzer funktioniert, wenn folgende Voraussetzungen erfüllt sind:

- Signiert in einem Windows-Gerät
- Die Benutzerkonto Domäne befindet sich in einer Windows Server 2012 R2-oder einer höheren Domänen Funktionsebene.

Geräteschutz für signierte geschützte Benutzer

Wenn der angemeldete Benutzer ein Mitglied der Gruppe "geschützte Benutzer" ist, werden die folgenden Schutzmaßnahmen angewendet:

- Bei der Delegierung von Gruppenrichtlinie Anmelde Informationen (aufwärtssp) werden die nur-Text-Anmelde Informationen des Benutzers nicht zwischengespeichert, auch wenn die Einstellung **Delegieren von Standard Anmelde Informationen zulassen** aktiviert ist.
- Ab Windows 8.1 und Windows Server 2012 R2 werden die nur-Text-Anmelde Informationen des Benutzers

von Windows Digest nicht zwischengespeichert, selbst wenn Windows Digest aktiviert ist.

NOTE

Nach der Installation der [Microsoft-Sicherheitsempfehlung 2871997](#) werden die Anmelde Informationen von Windows Digest weiterhin zwischengespeichert, bis der Registrierungsschlüssel konfiguriert wurde. Weitere Informationen finden Sie unter [Microsoft-Sicherheitsempfehlung: Update zum Verbessern von Anmelde Informationen Schutz und Verwaltung: 13. Mai 2014](#).

- NTLM speichert nicht die nur-Text-Anmelde Informationen des Benutzers oder die unidirektionale NT-Funktion (ntowf).
- Kerberos erstellt nicht mehr den-oder RC4-Schlüssel. Außerdem werden die nur-Text-Anmelde Informationen des Benutzers oder langfristige Schlüssel nicht zwischengespeichert, nachdem das erste TGT abgerufen wurde.
- Bei der Anmeldung oder beim Entsperren wird keine zwischengespeicherte Überprüfung erstellt, sodass die Offline Anmeldung nicht mehr unterstützt wird.

Nachdem das Benutzerkonto der Gruppe der geschützten Benutzer hinzugefügt wurde, beginnt der Schutz, wenn sich der Benutzer beim Gerät anmeldet.

Schutz von Domänen Controllern für geschützte Benutzer

Konten, die Mitglieder der Gruppe der geschützten Benutzer sind, die sich bei einer Windows Server 2012 R2-Domäne authentifizieren, können folgende Aktionen nicht ausführen:

- Authentifizieren mit NTLM-Authentifizierung.
- Verwenden von DES- oder RC4-Verschlüsselungstypen in Kerberos-Vorauthentifizierung.
- Delegation mit eingeschränkter oder nicht eingeschränkter Delegation.
- Erneuern der Kerberos-TGTs außerhalb der ursprünglichen Lebensdauer von vier Stunden.

Nicht konfigurierbare Einstellungen zum Ablauf von TGTs werden für jedes Konto in der Gruppe der geschützten Benutzer eingerichtet. Normalerweise legt der Domänencontroller die Lebensdauer und Erneuerung der TGTs basierend auf den Domänenrichtlinien fest, **Max. Gültigkeitsdauer des Benutzertickets** und **Max. Zeitraum, in dem ein Benutzerticket erneuert werden kann**. Für die Gruppe der geschützten Benutzer ist 600 Minuten für diese Domänenrichtlinien eingestellt.

Weitere Informationen finden Sie unter [Konfigurieren geschützter Konten](#).

Problembehandlung

Es gibt zwei betriebliche Administrativprotokolle für die Fehlerbehebung von Ereignissen hinsichtlich geschützter Benutzer. Diese neuen Protokolle befinden sich in Ereignisanzeige und sind standardmäßig deaktiviert und befinden sich unter **Anwendungs- und dienstprotokolle\microsoft\windows\authentication**.

| EREIGNIS-ID UND PROTOKOLL | BESCHREIBUNG |
|---------------------------|--------------|
|---------------------------|--------------|

| EREIGNIS-ID UND PROTOKOLL | BESCHREIBUNG |
|---|---|
| 104
ProtectedUser-Client | <p>Grund: Das Sicherheitspaket auf dem Client enthält keine Anmeldeinformationen.</p> <p>Der Fehler wird im Clientcomputer protokolliert, wenn das Konto Mitglied der Sicherheitsgruppe der geschützten Benutzer ist. Das Ereignis zeigt an, dass das Sicherheitspaket die Anmeldeinformationen, die für die Serverauthentifizierung erforderlich sind, nicht zwischenspeichert.</p> <p>Zeigt den Paketnamen, Benutzernamen, Domännennamen und den Servernamen an.</p> |
| 304
ProtectedUser-Client | <p>Grund: das Sicherheitspaket speichert nicht die Anmelde Informationen des geschützten Benutzers.</p> <p>Im Client wird ein Informations Ereignis protokolliert, um anzugeben, dass das Sicherheitspaket die Anmelde Informationen des Benutzers nicht zwischenspeichert. Es wird erwartet, dass Digest (WDigest), Delegierung von Anmeldeinformationen (CredSSP) und NTLM keine Anmeldeinformationen für geschützte Benutzer haben können. Anwendungen können weiterhin erfolgreich nach Anmeldeinformationen fragen.</p> <p>Zeigt den Paketnamen, Benutzernamen und Domännennamen an.</p> |
| 100
ProtectedUserFailures-DomainController | <p>Grund: Ein NTLM-Anmeldefehler ereignet sich für ein Konto in der Sicherheitsgruppe der geschützten Benutzer.</p> <p>Im Domänencontroller wird ein Fehler protokolliert, um anzugeben, dass die NTLM-Authentifizierung fehlgeschlagen ist, da das Konto Mitglied der Sicherheitsgruppe der geschützten Benutzer ist.</p> <p>Zeigt den Kontonamen und den Gerätenamen an.</p> |
| 104
ProtectedUserFailures-DomainController | <p>Grund: DES- oder RC4-Verschlüsselungstypen werden für die Kerberos-Authentifizierung verwendet, und ein Anmeldefehler ereignet sich für einen Benutzer in der Sicherheitsgruppe der geschützten Benutzer.</p> <p>Kerberos-Vorauthentifizierung ist fehlgeschlagen, da DES- und RC4-Verschlüsselungstypen nicht verwendet werden können, wenn das Konto Mitglied der Sicherheitsgruppe der geschützten Benutzer ist.</p> <p>(AES wird akzeptiert.)</p> |
| 303
ProtectedUserSuccesses-DomainController | <p>Grund: Ein Kerberos-Ticket-Granting-Ticket (TGT) wurde erfolgreich für ein Mitglied der Gruppe der geschützten Benutzer ausgegeben.</p> |

Weitere Ressourcen

- [Schutz und Verwaltung von Anmeldeinformationen](#)
- [Authentifizierungsrichtlinien und Authentifizierungsrichtliniensilos](#)
- [Konfigurieren geschützter Konten](#)

Authentifizierungsrichtlinien und Authentifizierungsrichtliniensilos

09.04.2020 • 34 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema für IT-Spezialisten werden Authentifizierungsrichtliniensilos und die Richtlinien beschrieben, mit denen Konten auf diese Silos beschränkt werden können. Zudem wird erklärt, wie der Bereich von Konten mit Authentifizierungsrichtlinien eingeschränkt werden kann.

Authentifizierungsrichtliniensilos und die zugehörigen Richtlinien stellen eine Möglichkeit dar, Anmeldeinformationen mit erhöhten Rechten auf Systeme zu beschränken, die nur für ausgewählte Benutzer, Computer oder Dienste relevant sind. Silos können mithilfe der Active Directory-Verwaltungscenter und der Active Directory Windows PowerShell-Cmdlets in Active Directory Domain Services (AD DS) definiert und verwaltet werden.

Authentifizierungsrichtliniensilos sind Container, denen Administratoren Benutzerkonten, Computerkonten und Dienstkonten zuweisen können. Über die Authentifizierungsrichtlinien, die auf diesen Container angewendet werden, können dann Gruppen von Konten verwaltet werden. Daher muss der Administrator nicht mehr im gleichen Umfang wie bisher den Ressourcenzugriff einzelner Konten verfolgen, und es wird verhindert, dass böswillige Benutzer durch den Diebstahl von Anmeldeinformationen Zugriff auf andere Ressourcen erlangen.

In Windows Server 2012 R2 eingeführte Funktionen ermöglichen es Ihnen, Authentifizierungs Richtlinien Silos zu erstellen, die eine Gruppe von Benutzern mit hohen Berechtigungen hosten. Sie können diesem Container Authentifizierungsrichtlinien zuordnen, um die Verwendung privilegierter Konten in der Domäne zu begrenzen. Wenn Konten zur Sicherheitsgruppe "Geschützte Benutzer" gehören, werden zusätzliche Kontrollmechanismen angewendet, z. B. die exklusive Verwendung des Kerberos-Protokolls.

Damit können Sie die Nutzung hochwertiger Konten auf hochwertige Hosts begrenzen. Beispielsweise könnten Sie ein neues Silo für Administratoren der Gesamtstruktur erstellen, das Unternehmens-, Schema- und Domänenadministratoren enthält. Anschließend könnten Sie das Silo mit einer Authentifizierungsrichtlinie konfigurieren, sodass eine kennwort- und smartcard-basierte Authentifizierung von Systemen, die keine Domänencontroller oder Domänenadministratorkonsolen sind, fehlschlägt.

Informationen zum Konfigurieren von Authentifizierungsrichtliniensilos und Authentifizierungsrichtlinien finden Sie unter [Konfigurieren geschützter Konten](#).

Informationen zu Authentifizierungsrichtliniensilos

Mit einem Authentifizierungsrichtliniensilo wird gesteuert, welche Konten durch das Silo eingeschränkt werden können, und es werden damit die Authentifizierungsrichtlinien definiert, die auf die Mitglieder angewendet werden sollen. Sie können das Silo anhand der Anforderungen Ihrer Organisation erstellen. Silos sind Active Directory-Objekte für Benutzer, Computer und Dienste, die nach dem Schema in der folgenden Tabelle definiert sind.

Active Directory Schema für Authentifizierungs Richtlinien Silos

| ANZEIGENAME | BESCHREIBUNG |
|-------------|--------------|
|-------------|--------------|

| ANZEIGENAME | BESCHREIBUNG |
|---|--|
| Authentifizierungsrichtliniensilo | Eine Instanz dieser Klasse definiert die Authentifizierungsrichtlinien und das zugehörige Verhalten für die zugewiesenen Benutzer, Computer und Dienste. |
| Authentifizierungsrichtliniensilos | Ein Container dieser Klasse kann Authentifizierungsrichtliniensilo-Objekte enthalten. |
| Authentication Policy Silo Enforced
(Authentifizierungsrichtliniensilo erzwungen) | Gibt an, ob das Authentifizierungsrichtliniensilo erzwungen wird.

Wenn es nicht erzwungen wird, dann ist für die Richtlinie standardmäßig der Überwachungsmodus aktiviert. Es werden Ereignisse generiert, die potenzielle Erfolge und Fehler anzeigen, aber es werden keine Schutzmaßnahmen auf das System angewendet. |
| Assigned Authentication Policy Silo Backlink (Rückverweis für zugewiesenes Authentifizierungsrichtliniensilo) | Dieses Attribut ist der Rückverweis für msDS-AssignedAuthNPolicySilo. |
| Authentication Policy Silo Members
(Authentifizierungsrichtliniensilo-Mitglieder) | Gibt an, welche Prinzipale dem AuthNPolicySilo-Objekt zugewiesen sind. |
| Authentication Policy Silo Members Backlink (Rückverweis für Authentifizierungsrichtliniensilo-Mitglieder) | Dieses Attribut ist der Rückverweis für msDS-AuthNPolicySiloMembers. |

Authentifizierungsrichtliniensilos können mit der Active Directory-Verwaltungskonsole oder Windows PowerShell konfiguriert werden. Weitere Informationen finden Sie unter [Konfigurieren geschützter Konten](#).

Informationen zu Authentifizierungsrichtlinien

Authentifizierungsrichtlinien definieren die Lebensdauereigenschaften des Ticket-Granting Ticket (TGT) für das Kerberos-Protokoll und die Bedingungen für die Authentifizierungszugriffssteuerung für einen Kontotyp. Die Richtlinie basiert auf und steuert den AD DS Container, der als Authentifizierungs Richtlinien Silo bezeichnet wird.

Über Authentifizierungsrichtlinien wird Folgendes gesteuert:

- Die TGT-Lebensdauer des Kontos, das als nicht erneuerbar konfiguriert wurde.
- Die Kriterien, die Gerätekonten erfüllen müssen, um sich mit einem Kennwort oder einem Zertifikat anmelden zu können.
- Die Kriterien, die Benutzer und Geräte erfüllen müssen, um sich gegenüber Diensten authentifizieren zu können, die unter dem Konto ausgeführt werden.

Der Active Directory Kontotyp bestimmt die Rolle des Aufrufers als einer der folgenden:

- **User**

Benutzer sollten immer Mitglied der Sicherheitsgruppe "Geschützte Benutzer" sein, die Authentifizierungsversuche über NTLM standardmäßig nicht zulässt.

Richtlinien können so konfiguriert werden, dass die TGT-Lebensdauer eines Benutzerkontos auf einen kürzeren Wert festgelegt wird oder die Geräte eingeschränkt werden, auf die sich ein Benutzerkonto anmelden kann. Rich-Ausdrücke können in der Authentifizierungs Richtlinie konfiguriert werden, um die Kriterien zu steuern, die die Benutzer und Ihre Geräte erfüllen müssen, um sich beim Dienst zu authentifizieren.

Weitere Informationen finden Sie unter [Sicherheitsgruppe "Geschützte Benutzer"](#).

- **Dienst**

Eigenständige verwaltete Dienstkonten, gruppenverwalteten Dienstkonten oder ein benutzerdefiniertes Kontoobjekt, das von diesen beiden Dienstkontotypen abgeleitet ist, werden verwendet. Mit Richtlinien können die Zugriffs Steuerungs Bedingungen eines Geräts festgelegt werden, die verwendet werden, um die Anmelde Informationen für verwaltete Dienst Konten auf bestimmte Geräte mit einer Active Directory-Identität einzuschränken. Dienste sollten nie Mitglied der Sicherheitsgruppe "Geschützte Benutzer" sein, weil sonst alle eingehenden Authentifizierungsversuche fehlschlagen.

- **Computer**

Verwendet wird das Computerkontoobjekt oder das benutzerdefinierte Kontoobjekt, das vom Computerkontoobjekt abgeleitet wurde. Durch Richtlinien können die Zugriffssteuerungsbedingungen festgelegt werden, die erfüllt sein müssen, um eine Authentifizierung anhand der Benutzer- oder Geräteeigenschaften gegenüber dem Konto zuzulassen. Computer sollten nie Mitglied der Sicherheitsgruppe "Geschützte Benutzer" sein, weil sonst alle eingehenden Authentifizierungsversuche fehlschlagen. Standardmäßig werden NTLM-Authentifizierungsversuche abgelehnt. Für Computerkonten sollte keine TGT-Lebensdauer konfiguriert werden.

NOTE

Es ist möglich, eine Authentifizierungsrichtlinie für eine Gruppe von Konten festzulegen, ohne die Richtlinie mit einem Authentifizierungsrichtliniensilo zu verknüpfen. Sie können diese Strategie verwenden, wenn nur ein einzelnes Konto geschützt werden muss.

Active Directory Schema für Authentifizierungs Richtlinien

Die Richtlinien für die Active Directory-Objekte für Benutzer, Computer und Dienste werden nach dem Schema in der folgenden Tabelle definiert.

| TYP | ANZEIGENAME | BESCHREIBUNG |
|---------------------|--|---|
| Policy (Richtlinie) | Authentifizierungsrichtlinie | Eine Instanz dieser Klasse definiert Authentifizierungsrichtlinienverhalten für die zugewiesenen Prinzipale. |
| Policy (Richtlinie) | Authentifizierungsrichtlinien | Ein Container dieser Klasse kann Authentifizierungsrichtlinien-Objekte enthalten. |
| Policy (Richtlinie) | Authentication Policy Enforced (Authentifizierungsrichtlinien erzwungen) | Gibt an, ob die Authentifizierungsrichtlinie erzwungen wird.

Wenn sie nicht erzwungen wird, dann ist für die Richtlinie standardmäßig der Überwachungsmodus aktiviert, und es werden Ereignisse zum Anzeigen potenzieller Erfolge oder Fehler generiert, aber keine Schutzmaßnahmen auf das System angewendet. |
| Policy (Richtlinie) | Assigned Authentication Policy Backlink (Rückverweis für zugewiesene Authentifizierungsrichtlinie) | Dieses Attribut ist der Rückverweis für msDS-AssignedAuthNPolicy. |

| TYP | ANZEIGENAME | BESCHREIBUNG |
|---------------------|---|--|
| Policy (Richtlinie) | Assigned Authentication Policy
(Zugewiesene Authentifizierungsrichtlinie) | Gibt an, welches AuthNPolicy-Objekt auf diesen Prinzipal angewendet werden soll. |
| Benutzer | User Authentication Policy
(Benutzerauthentifizierungsrichtlinie) | Gibt an, welches AuthNPolicy-Objekt auf die Benutzer, die diesem Siloobjekt zugewiesen wurden, angewendet werden soll. |
| Benutzer | User Authentication Policy Backlink
(Rückverweis für Benutzerauthentifizierungsrichtlinie) | Dieses Attribut ist der Rückverweis für msDS-UserAuthNPolicy. |
| Benutzer | ms-DS-User-Allowed-To-Authenticate-To | Mit diesem Attribut wird bestimmt, welcher Gruppe von Prinzipalen erlaubt wird, sich gegenüber einem Dienst, der unter dem Benutzerkonto ausgeführt wird, zu authentifizieren. |
| Benutzer | ms-DS-User-Allowed-To-Authenticate-From | Mit diesem Attribut wird die Gruppe von Geräten festgelegt, für die ein Benutzerkonto Anmeldeberechtigungen besitzt. |
| Benutzer | User TGT Lifetime (Benutzer-TGT-Lebensdauer) | Legt das maximale Alter (in Sekunden) eines Kerberos-TGT fest, das für einen Benutzer ausgestellt wird. Die resultierenden TGTs sind nicht erneuerbar. |
| Computer | Computer Authentication Policy
(Computerauthentifizierungsrichtlinie) | Gibt an, welches AuthNPolicy-Objekt auf die Computer, die diesem Siloobjekt zugewiesen wurden, angewendet werden soll. |
| Computer | Computer Authentication Policy Backlink
(Rückverweis für Computerauthentifizierungsrichtlinie) | Dieses Attribut ist der Rückverweis für msDS-ComputerAuthNPolicy. |
| Computer | ms-DS-Computer-Allowed-To-Authenticate-To | Mit diesem Attribut wird bestimmt, welcher Gruppe von Prinzipalen erlaubt wird, sich gegenüber einem Dienst, der unter dem Computerkonto ausgeführt wird, zu authentifizieren. |
| Computer | Computer TGT Lifetime (Computer-TGT-Lebensdauer) | Legt das maximale Alter (in Sekunden) eines Kerberos-TGT fest, das für einen Computer ausgestellt wird. Von der Änderung dieser Einstellung wird abgeraten. |
| Service | Service Authentication Policy
(Dienstauthentifizierungsrichtlinie) | Gibt an, welches AuthNPolicy-Objekt auf die Dienste, die diesem Siloobjekt zugewiesen wurden, angewendet werden soll. |

| TYP | ANZEIGENAME | BESCHREIBUNG |
|---------|---|--|
| Service | Service Authentication Policy Backlink
(Rückverweis für
Dienstauthentifizierungsrichtlinie) | Dieses Attribut ist der Rückverweis für
msDS-ServiceAuthNPolicy. |
| Service | ms-DS-Service-Allowed-To-
Authenticate-To | Mit diesem Attribut wird bestimmt,
welcher Gruppe von Prinzipalen erlaubt
wird, sich gegenüber einem Dienst, der
unter dem Dienstkonto ausgeführt
wird, zu authentifizieren. |
| Service | ms-DS-Service-Allowed-To-
Authenticate-From | Mit diesem Attribut wird die Gruppe
von Geräten festgelegt, für die ein
Dienstkonto Anmeldeberechtigungen
besitzt. |
| Service | Service TGT Lifetime (Dienst-TGT-
Lebensdauer) | Legt das maximale Alter (in Sekunden)
eines Kerberos-TGT fest, das für einen
Dienst ausgestellt wird. |

Authentifizierungsrichtlinien können mit der Active Directory-Verwaltungskonsolle oder Windows PowerShell für jedes Silo konfiguriert werden. Weitere Informationen finden Sie unter [Konfigurieren geschützter Konten](#).

So funktioniert's

In diesem Abschnitt wird die Funktionsweise von Authentifizierungsrichtliniensilos und Authentifizierungsrichtlinien in Verbindung mit der Sicherheitsgruppe "Geschützte Benutzer" und die Implementierung des Kerberos-Protokolls in Windows beschrieben.

- [Verwendung des Kerberos-Protokolls mit Authentifizierungsilos und-Richtlinien](#)
- [Funktionsweise der Benutzeranmeldung](#)
- [Funktionsweise der Dienst Ticket Ausstellung](#)

Geschützte Konten

Die Sicherheitsgruppe "geschützte Benutzer" löst nicht konfigurierbaren Schutz auf Geräten und Host Computern aus, auf denen Windows Server 2012 R2 und Windows 8.1 ausgeführt wird, sowie auf Domänen Controllern in Domänen mit einem primären Domänen Controller unter Windows Server 2012 R2. Abhängig von der Domänenfunktionsebene des Kontos sind die Mitglieder der Sicherheitsgruppe "Geschützte Benutzer" aufgrund der Änderungen der Authentifizierungsmethoden, die in Windows unterstützt werden, zusätzlich geschützt.

- Mitglieder der Sicherheitsgruppe "Geschützte Benutzer" können sich nicht unter Verwendung von NTLM, Digestauthentifizierung oder der Delegierung der Standardanmeldeinformationen mit CredSSP authentifizieren. Auf einem Gerät mit Windows 8.1, das einen dieser SSPs (Security Support Providers) verwendet, schlägt die Authentifizierung bei einer Domäne fehl, wenn das Konto Mitglied der Sicherheitsgruppe "geschützte Benutzer" ist.
- Das Kerberos-Protokoll verwendet die schwächeren Verschlüsselungstypen DES oder RC4 nicht im Vorauthentifizierungsprozess. Daher muss die Domäne so konfiguriert werden, dass mindestens der Verschlüsselungstyp AES unterstützt wird.
- Das Konto des Benutzers kann nicht mit eingeschränkter oder nicht eingeschränkter Kerberos-Delegierung delegiert werden. Das bedeutet, dass frühere Verbindungen mit anderen Systemen fehlschlagen, wenn der Benutzer Mitglied der Sicherheitsgruppe "Geschützte Benutzer" ist.

- Die Standardeinstellung für die Lebensdauer von Kerberos-TGTs von vier Stunden kann mit Authentifizierungsrichtlinien und -silos konfiguriert werden, auf die über das Active Directory-Verwaltungszentrum zugegriffen werden kann. Das heißt, dass sich der Benutzer nach Ablauf von vier Stunden erneut authentifizieren muss.

Weitere Informationen zu dieser Sicherheitsgruppe finden Sie unter [Funktionsweise der Gruppe "Geschützte Benutzer"](#).

Silos und Authentifizierungs Richtlinien

Authentifizierungsrichtliniensilos und Authentifizierungsrichtlinien nutzen die vorhandene Windows-Authentifizierungsinfrastruktur. Die Verwendung des NTLM-Protokolls wird abgelehnt, und das Kerberos-Protokoll wird mit neueren Verschlüsselungstypen verwendet. Authentifizierungsrichtlinien ergänzen die Sicherheitsgruppe "Geschützte Benutzer" durch die Möglichkeit, konfigurierbare Einschränkungen auf Konten anzuwenden, sowie durch die Bereitstellung von Einschränkungen für Dienst- und Computerkonten. Authentifizierungsrichtlinien werden während des Austauschs des Authentifizierungsdiensts (Authentication Service, AS) und des Ticket-Granting Service (TGS) des Kerberos-Protokolls erzwungen. Weitere Informationen dazu, wie Windows das Kerberos-Protokoll verwendet und welche Änderungen zur Unterstützung von Authentifizierungsrichtliniensilos und Authentifizierungsrichtlinien vorgenommen wurden, finden Sie unter:

- [Funktionsweise des Kerberos Version 5-Authentifizierungs Protokolls](#)
- [Änderungen bei der Kerberos-Authentifizierung](#) (Windows Server 2008 R2 und Windows 7)

Verwendung des Kerberos-Protokolls mit Authentifizierungs Richtlinien Silos und-Richtlinien

Wenn ein Domänenkonto mit einem Authentifizierungsrichtliniensilo verknüpft wird und der Benutzer sich anmeldet, fügt der Sicherheitskonto-Manager den Anspruchstyp "Authentifizierungsrichtliniensilo" hinzu, der das Silo als Wert enthält. Dieser Anspruch im Konto bietet Zugriff auf das betreffende Silo.

Wenn eine Authentifizierungsrichtlinie erzwungen wird und die Authentifizierungsdienstanforderung für ein Domänenkonto beim Domänencontroller eingeht, dann gibt der Domänencontroller ein nicht erneuerbares TGT mit der konfigurierten Lebensdauer zurück (sofern das Domänen-TGT keine kürzere Lebensdauer hat).

NOTE

Das Domänenkonto muss eine konfigurierte TGT-Lebensdauer besitzen und entweder direkt oder indirekt über die Silomitgliedschaft mit der Richtlinie verknüpft werden.

Wenn der Überwachungsmodus für eine Authentifizierungsrichtlinie aktiviert ist und beim Domänencontroller die Authentifizierungsdienstanforderung für ein Domänenkonto eingeht, dann prüft der Domänencontroller, ob die Authentifizierung des Geräts zulässig ist, damit beim Auftreten eines Fehlers eine Warnung protokolliert werden kann. Da der Prozess durch eine überwachte Authentifizierungsrichtlinie nicht geändert wird, schlagen Authentifizierungsanforderungen nicht fehl, wenn sie die Anforderungen der Richtlinie nicht erfüllen.

NOTE

Das Domänenkonto muss entweder direkt oder indirekt über die Silomitgliedschaft mit der Richtlinie verknüpft werden.

Wenn eine Authentifizierungsrichtlinie erzwungen wird und der Authentifizierungsdienst Kerberos Armoring verwendet, dann wird die Authentifizierungsdienstanforderung für ein Domänenkonto auf dem Domänencontroller empfangen, und der Domänencontroller prüft, ob die Authentifizierung für das Gerät zulässig ist. Wenn ein Fehler auftritt, gibt der Domänencontroller eine Fehlermeldung zurück und protokolliert ein Ereignis.

NOTE

Das Domänenkonto muss entweder direkt oder indirekt über die Silomitgliedschaft mit der Richtlinie verknüpft werden.

Wenn sich eine Authentifizierungs Richtlinie im Überwachungsmodus befindet und ein Ticket Erstellungs Service Request vom Domänen Controller für ein Domänen Konto empfangen wird, prüft der Domänen Controller, ob die Authentifizierung gemäß den PAC-Daten (Ticket Privilege Attribute Certificate) der Anforderung zulässig ist, und protokolliert eine Warnmeldung, wenn ein Fehler auftritt. Das PAC enthält verschiedene Arten von Autorisierungsdaten, darunter die Gruppen, denen der Benutzer als Mitglied angehört, die Rechte des Benutzers und die Richtlinien, die für den Benutzer gelten. Diese Informationen werden verwendet, um das Zugriffs Token des Benutzers zu generieren. Handelt es sich um eine erzwungene Authentifizierungs Richtlinie, die die Authentifizierung für einen Benutzer, ein Gerät oder einen Dienst ermöglicht, prüft der Domänen Controller, ob die Authentifizierung auf der Grundlage der PAC-Daten der Anforderung zulässig ist. Wenn ein Fehler auftritt, gibt der Domänencontroller eine Fehlermeldung zurück und protokolliert ein Ereignis.

NOTE

Das Domänenkonto muss entweder direkt oder indirekt über die Silomitgliedschaft mit einer überwachten Richtlinie verknüpft werden, welche die Authentifizierung eines Benutzers, Geräts oder Diensts zulässt.

Sie können eine Authentifizierungsrichtlinie für alle Mitglieder eines Silos oder getrennte Richtlinien für Benutzer, Computer und verwaltete Dienstkonto verwenden.

Authentifizierungsrichtlinien können mit der Active Directory-Verwaltungskonsolle oder Windows PowerShell für jedes Silo konfiguriert werden. Weitere Informationen finden Sie unter [Konfigurieren geschützter Konten](#).

Funktionsweise der Benutzeranmeldung

Weil diese Authentifizierungsrichtlinien auf ein Konto angewendet werden, gelten sie auch für Konten, die von Diensten verwendet werden. Wenn Sie die Verwendung eines Kennworts für einen Dienst auf bestimmte Hosts beschränken möchten, ist diese Einstellung hilfreich. Beispielsweise werden gruppenverwaltete Dienstkonto so konfiguriert, dass die Hosts das Kennwort von den Active Directory-Domänendiensten abrufen können. Allerdings kann dieses Kennwort auf jedem Host zur anfänglichen Authentifizierung verwendet werden. Durch die Anwendung einer Zugriffssteuerungsbedingung kann eine zusätzliche Schutzebene eingeführt werden, indem das Kennwort nur auf die Gruppe von Hosts begrenzt wird, welche das Kennwort abrufen können.

Wenn von Diensten, die als System, Netzwerkdienst oder andere Identität des lokalen Diensts ausgeführt werden, eine Verbindung mit Netzwerkdiensten hergestellt wird, wird das Computer Konto des Hosts verwendet. Computerkonten können nicht beschränkt werden. Selbst wenn der Dienst ein Computerkonto verwendet, das nicht für einen Windows-Host vorgesehen ist, kann dieses nicht eingeschränkt werden.

Wenn Sie die Benutzeranmeldung auf bestimmte Hosts einschränken, muss der Domänen Controller die Identität des Hosts überprüfen. Bei Verwendung der Kerberos-Authentifizierung mit Kerberos Amoring (die Bestandteil der dynamischen Zugriffssteuerung ist), dann wird das Schlüsselverteilungscenter mit dem TGT des Hosts bereitgestellt, von dem der Benutzer authentifiziert wird. Der Inhalt dieses geschützten TGT wird zur Durchführung einer Zugriffsprüfung verwendet, mit der bestimmt wird, ob der Host zulässig ist.

Wenn sich der Benutzer bei Windows anmeldet oder seine Domänenanmeldeinformationen in eine Eingabeaufforderung für die Anmeldung bei einer Anwendung eingibt, dann sendet Windows standardmäßig eine ungeschützte Authentifizierungsdienstanforderung (AS-REQ) an den Domänencontroller. Wenn der Benutzer die Anforderung von einem Computer sendet, der keine hoch Rüstung unterstützt (z. b. Computer mit Windows 7 oder Windows Vista), schlägt die Anforderung fehl.

In der folgenden Liste wird der Prozess beschrieben:

- Der Domänen Controller in einer Domäne, auf der Windows Server 2012 R2 ausgeführt wird, fragt das Benutzerkonto ab und bestimmt, ob es mit einer Authentifizierungs Richtlinie konfiguriert ist, die die anfängliche Authentifizierung einschränkt, die hochgerüstete Anforderungen erfordert.
- Der Domänencontroller kann die Anforderung nicht erfüllen.
- Da armoring erforderlich ist, kann der Benutzer versuchen, sich mit einem Computer anzumelden, auf dem Windows 8.1 oder Windows 8 ausgeführt wird, der Kerberos armoring unterstützen kann, um den Anmeldevorgang zu wiederholen.
- Windows erkennt, dass die Domäne Kerberos Armoring unterstützt, und sendet eine geschützte AS-REQ, um die Anmeldungsanforderung zu wiederholen.
- Der Domänen Controller führt eine Zugriffs Überprüfung mit den konfigurierten Zugriffs Steuerungs Bedingungen und den Identitätsinformationen des Client Betriebssystems im TGT aus, die zur Rüstung der Anforderung verwendet wurden.
- Wenn die Zugriffsprüfung fehlschlägt, lehnt der Domänencontroller die Anforderung ab.

Selbst wenn das Betriebssystem Kerberos Armoring unterstützt, können Zugriffssteuerungsanforderungen angewendet werden, die erfüllt sein müssen, bevor der Zugriff gewährt wird. Die Benutzer melden sich bei Windows an oder geben ihre Domänenanmeldeinformationen in eine Eingabeaufforderung für die Anmeldung bei einer Anwendung ein. Standardmäßig sendet Windows eine ungeschützte AS-REQ an den Domänencontroller. Wenn der Benutzer die Anforderung von einem Computer sendet, der armoring unterstützt (z. b. Windows 8.1 oder Windows 8), werden Authentifizierungs Richtlinien wie folgt ausgewertet:

1. Der Domänen Controller in einer Domäne, auf der Windows Server 2012 R2 ausgeführt wird, fragt das Benutzerkonto ab und bestimmt, ob es mit einer Authentifizierungs Richtlinie konfiguriert ist, die die anfängliche Authentifizierung einschränkt, die hochgerüstete Anforderungen erfordert.
2. Der Domänen Controller führt eine Zugriffs Überprüfung mithilfe der konfigurierten Zugriffs Steuerungs Bedingungen und der Identitätsinformationen des Systems im TGT aus, die zur Rüstung der Anforderung verwendet werden. Die Zugriffsprüfung ist erfolgreich.

NOTE

Wenn ältere Arbeitsgruppeneinschränkungen konfiguriert wurden, müssen auch diese erfüllt werden.

3. Der Domänencontroller antwortet mit einer geschützten Antwort (AS-REP), und die Authentifizierung wird fortgesetzt.

Funktionsweise der Dienst Ticket Ausstellung

Wenn ein Konto nicht zulässig ist und ein Benutzer, der ein TGT verwendet, eine Verbindung mit dem Dienst herstellt (z. b. durch Öffnen einer Anwendung, die eine Authentifizierung bei einem Dienst erfordert, der durch den Dienst Prinzipal Namen (SPN) des Dienstanbieter identifiziert wird, erfolgt die folgende Sequenz:

1. Bei einem Versuch, von SPN eine Verbindung mit SPN1 herzustellen, sendet Windows eine TGS-REQ an den Domänencontroller, der ein Dienstticket für SPN1 anfordert.
2. Der Domänen Controller in einer Domäne, auf der Windows Server 2012 R2 ausgeführt wird, sucht nach dem Active Directory Domain Services Konto für den Dienst und stellt fest, dass das Konto mit einer Authentifizierungs Richtlinie konfiguriert ist, die die Ausstellung von Dienst Tickets einschränkt.
3. Der Domänen Controller führt eine Zugriffs Überprüfung mit den konfigurierten Zugriffs Steuerungs Bedingungen und den Identitätsinformationen des Benutzers im TGT aus. Die Zugriffsprüfung schlägt fehl.
4. Der Domänencontroller weist die Anforderung zurück.

Wenn ein Konto zulässig ist, weil das Konto die von der Authentifizierungs Richtlinie festgelegten Zugriffs Steuerungs Bedingungen erfüllt und ein Benutzer, der ein TGT hat, versucht, eine Verbindung mit dem Dienst herzustellen (z. b. durch Öffnen einer Anwendung, die eine Authentifizierung bei einem Dienst erfordert, der durch den Dienst Prinzipal Namen identifiziert wird), erfolgt die folgende Sequenz:

1. Bei einem Versuch, eine Verbindung mit SPN1 herzustellen, sendet Windows eine TGS-REQ an den Domänencontroller, der ein Dienstticket für SPN1 anfordert.
2. Der Domänen Controller in einer Domäne, auf der Windows Server 2012 R2 ausgeführt wird, sucht nach dem Active Directory Domain Services Konto für den Dienst und stellt fest, dass das Konto mit einer Authentifizierungs Richtlinie konfiguriert ist, die die Ausstellung von Dienst Tickets einschränkt.
3. Der Domänen Controller führt eine Zugriffs Überprüfung mit den konfigurierten Zugriffs Steuerungs Bedingungen und den Identitätsinformationen des Benutzers im TGT aus. Die Zugriffsprüfung ist erfolgreich.
4. Der Domänencontroller beantwortet die Anforderung mit einer Ticket erteilenden Dienstantwort (TGS-REP).

Zugehörige Fehler-und Informations Ereignismeldungen

In der folgenden Tabelle werden die Ereignisse, die mit der Sicherheitsgruppe "Geschützte Benutzer" zusammenhängen, und die Authentifizierungsrichtlinien, die für Authentifizierungsrichtliniensilos gelten, beschrieben.

Die Ereignisse werden in den Anwendungs- und Dienstprotokollen unter **Microsoft\Windows\Authentication** verzeichnet.

Informationen zu Problembehandlungsschritten mit diesen Ereignissen finden Sie unter [Problembehandlung von Authentifizierungsrichtlinien](#) und [Problembehandlungen von Ereignissen im Zusammenhang mit geschützten Benutzern](#).

| EREIGNIS-ID UND PROTOKOLL | BESCHREIBUNG |
|---|--|
| 101
AuthenticationPolicyFailures-DomainController | <p>Grund: ein NTLM-Anmeldefehler tritt auf, weil die Authentifizierungs Richtlinie konfiguriert ist.</p> <p>Auf dem Domänencontroller wird ein Ereignis protokolliert, das anzeigt, dass die NTLM-Authentifizierung fehlgeschlagen ist, weil Zugriffssteuerungseinschränkungen erfüllt werden müssen und diese Einschränkungen nicht auf NTLM anwendbar sind.</p> <p>Zeigt den Kontonamen, Gerätenamen, Richtliniennamen und Silonamen an.</p> |
| 105
AuthenticationPolicyFailures-DomainController | <p>Ursache: ein Kerberos-Einschränkungs Fehler tritt auf, weil die Authentifizierung von einem bestimmten Gerät nicht zugelassen wurde.</p> <p>Auf dem Domänencontroller wird ein Ereignis protokolliert, das anzeigt, dass ein Kerberos-TGT verweigert wurde, weil das Gerät nicht die erzwungenen Zugriffssteuerungseinschränkungen erfüllte.</p> <p>Zeigt Kontonamen, Gerätenamen, Richtliniennamen, Silonamen und TGT-Lebensdauer an.</p> |

| EREIGNIS-ID UND PROTOKOLL | BESCHREIBUNG |
|--|---|
| <p>305</p> <p>AuthenticationPolicyFailures-DomainController</p> | <p>Ursache: Möglicherweise tritt ein potenzieller Kerberos-Einschränkungs Fehler auf, weil die Authentifizierung von einem bestimmten Gerät nicht zugelassen wurde.</p> <p>Im Überwachungsmodus wird auf dem Domänencontroller ein Ereignis protokolliert, das anzeigt, dass ein Kerberos-TGT verweigert wurde, weil das Gerät nicht die erzwungenen Zugriffssteuerungseinschränkungen erfüllt.</p> <p>Zeigt Kontonamen, Gerätenamen, Richtliniennamen, Silonamen und TGT-Lebensdauer an.</p> |
| <p>106</p> <p>AuthenticationPolicyFailures-DomainController</p> | <p>Ursache: ein Kerberos-Einschränkungs Fehler tritt auf, weil der Benutzer oder das Gerät nicht für die Authentifizierung beim Server berechtigt war.</p> <p>Auf dem Domänencontroller wird ein Ereignis protokolliert, das anzeigt, dass ein Kerberos-Dienstticket verweigert wurde, weil der Benutzer, das Gerät oder beide nicht die erzwungenen Zugriffssteuerungseinschränkungen erfüllen.</p> <p>Zeigt den Gerätenamen, Richtliniennamen und Silonamen an.</p> |
| <p>306</p> <p>AuthenticationPolicyFailures-DomainController</p> | <p>Ursache: Möglicherweise tritt ein Kerberos-Einschränkungs Fehler auf, weil der Benutzer oder das Gerät nicht auf dem Server authentifiziert werden darf.</p> <p>Im Überwachungsmodus wird auf dem Domänencontroller ein Ereignis protokolliert, das anzeigt, dass ein Kerberos-Dienstticket verweigert wurde, weil der Benutzer, das Gerät oder beide nicht die Zugriffssteuerungseinschränkungen erfüllen.</p> <p>Zeigt den Gerätenamen, Richtliniennamen und Silonamen an.</p> |

Siehe auch

[Konfigurieren geschützter Konten](#)

[Schutz und Verwaltung von Anmeldeinformationen](#)

[Sicherheitsgruppe „Geschützte Benutzer“](#)

Group Managed Service Accounts Overview

09.04.2020 • 6 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema für IT-Experten wird das Gruppen verwaltete Dienst Konto eingeführt. hierzu werden praktische Anwendungen, Änderungen in der Implementierung von Microsoft sowie Hardware-und Softwareanforderungen beschrieben.

Featurebeschreibung

Ein eigenständiges verwaltetes Dienst Konto (Managed Service Account, SMSA) ist ein verwaltetes Domänen Konto, das die automatische Kenn Wort Verwaltung, vereinfachte Dienst Prinzipal Namen-Verwaltung (Service Principal Name, SPN) und die Möglichkeit zum Delegieren der Verwaltung Diese Art von verwaltetem Dienst Konto (MSA) wurde in Windows Server 2008 R2 und Windows 7 eingeführt.

Das Gruppen verwaltete Dienst Konto (Group Managed Service Account, GMSA) bietet die gleiche Funktionalität innerhalb der Domäne, erweitert diese Funktionalität aber auch auf mehrere Server. Beim Herstellen einer Verbindung mit einem auf einer Serverfarm gehosteten Dienst, wie z. b. der Lösung für Netzwerk Lastenausgleich, erfordern die Authentifizierungsprotokolle, die gegenseitige Authentifizierung unterstützen, dass alle Instanzen der Dienste denselben Prinzipal Wenn ein GMSA als Dienst Prinzipale verwendet wird, verwaltet das Windows-Betriebssystem das Kennwort für das Konto, anstatt sich auf den Administrator zu verlassen, um das Kennwort zu verwalten.

Der Microsoft-Schlüssel Verteilungsdienst (kdsv. dll) stellt den Mechanismus zum sicheren Abrufen des aktuellen Schlüssels oder eines bestimmten Schlüssels mit einer Schlüssel Kennung für ein Active Directory Konto bereit. Vom Schlüsselverteilungsdienst werden geheime Informationen zur Erstellung von Schlüsseln für das Konto bereitgestellt. Diese Schlüssel werden regelmäßig geändert. Bei einem GMSA berechnet der Domänen Controller das Kennwort für den Schlüssel, der von den Schlüssel Verteilung Diensten bereitgestellt wird, zusätzlich zu anderen Attributen des GMSA. Mitglieder Hosts können die aktuellen und vorangehenden Kenn Wort Werte abrufen, indem Sie einen Domänen Controller kontaktieren.

Praktische Anwendungen

gmsas bieten eine einzelne Identitäts Lösung für Dienste, die in einer Serverfarm oder auf Systemen hinter Netzwerk Load Balancer ausgeführt werden. Durch die Bereitstellung einer GMSA-Lösung können Dienste für den neuen GMSA-Prinzipal konfiguriert werden, und die Kenn Wort Verwaltung wird von Windows verarbeitet.

Durch die Verwendung eines GMSA müssen Dienste oder Dienst Administratoren die Kenn Wort Synchronisierung zwischen Dienst Instanzen nicht verwalten. Das GMSA unterstützt Hosts, die über einen längeren Zeitraum offline gehalten werden, sowie die Verwaltung von Mitglieds Hosts für alle Instanzen eines Diensts. Sie können also eine Serverfarm bereitstellen, die eine einzelne Identität unterstützt, gegenüber der sich vorhandene Clientcomputer authentifizieren können, ohne zu wissen, mit welcher Instanz des Diensts eine Verbindung hergestellt wird.

Failovercluster unterstützen keine gruppenverwalteten Dienstkonten. Dienste, die oben im Clusterdienst ausgeführt werden, können jedoch ein gMSA oder sMSA verwenden, wenn sie ein Windows-Dienst, ein App-Pool, eine geplante Aufgabe oder gMSA oder sMSA systemeigen unterstützen.

Software Anforderungen

Zum Ausführen der Windows PowerShell-Befehle, die zur Verwaltung von gmsas verwendet werden, ist eine 64-Bit-Architektur erforderlich.

Ein verwaltetes Dienstkonto ist abhängig von Verschlüsselungstypen mit Kerberos-Unterstützung. Wenn sich ein Clientcomputer gegenüber einem Server per Kerberos authentifiziert, wird vom Domänencontroller ein Kerberos-Dienstticket erstellt, das mit einer Verschlüsselung geschützt ist, die sowohl vom Domänencontroller als auch vom Server unterstützt wird. Der Domänen Controller verwendet das msDS--supportedencryptiontypes-Attribut des Kontos, um zu bestimmen, welche Verschlüsselung der Server unterstützt. Wenn kein Attribut vorhanden ist, wird davon ausgegangen, dass der Client Computer stärkere Verschlüsselungstypen nicht unterstützt. Wenn der Host so konfiguriert ist, dass RC4 nicht unterstützt wird, tritt bei der Authentifizierung immer ein Fehler auf. Aus diesem Grund muss AES für verwaltete Dienstkonten immer explizit konfiguriert sein.

NOTE

Ab Windows Server 2008 R2 ist DES standardmäßig deaktiviert. Weitere Informationen zu den unterstützten Verschlüsselungsarten finden Sie unter [Changes in Kerberos Authentication](#).

gmsas gelten nicht für Windows-Betriebssysteme vor Windows Server 2012.

Informationen zum Server-Manager

Es sind keine Konfigurationsschritte erforderlich, um MSA und GMSA mithilfe von Server-Manager oder mit dem Cmdlet Install-Windows Feature zu implementieren.

Siehe auch

In der folgenden Tabelle sind Links zu weiterführenden Ressourcen im Zusammenhang mit verwalteten Dienstkonten und gruppenverwalteten Dienstkonten aufgeführt.

| ART DES INHALTS | VERWEISE |
|-------------------------|---|
| Produktbewertung | Neuerungen bei verwalteten Dienst Konten
Dokumentation zu verwalteten Dienst Konten für Windows 7 und Windows Server 2008 R2
Schritt Anleitung für Dienst Konten--Schritt Anleitung |
| Planung | Noch nicht verfügbar |
| Bereitstellung | Noch nicht verfügbar |
| Betrieb | Verwaltete Dienst Konten in Active Directory |
| Problembehandlung | Noch nicht verfügbar |
| Beurteilung | Erste Schritte mit gruppenverwalteten Dienstkonten |
| Tools und Einstellungen | Verwaltete Dienst Konten in Active Directory Domain Services |
| Communityressourcen | Verwaltete Dienst Konten: Grundlegendes, Implementierung, bewährte Methoden und Problembehandlung |
| Verwandte Technologien | Übersicht über Active Directory-Domänendienste |

Getting Started with Group Managed Service Accounts

22.05.2020 • 24 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016

Diese Anleitung enthält Schritt-für-Schritt-Anleitungen und Hintergrundinformationen zum Aktivieren und Verwenden von Gruppen verwalteten Dienst Konten in Windows Server 2012.

Inhalt dieses Dokuments

- [Erforderliche Komponenten](#)
- [Introduction \(Einführung\)](#)
- [Bereitstellen einer neuen Serverfarm](#)
- [Hinzufügen von Mitgliedshosts zu einer vorhandenen Serverfarm](#)
- [Aktualisieren der Eigenschaften für Gruppen verwaltete Dienst Konten](#)
- [Außerbetriebsetzung von Mitgliedshosts in einer vorhandenen Serverfarm](#)

NOTE

Dieses Thema enthält Windows PowerShell-Beispiel-Cmdlets, mit denen Sie einige der beschriebenen Vorgehensweisen automatisieren können. Weitere Informationen finden Sie unter [Verwenden von Cmdlets](#).

Voraussetzungen

Informationen finden Sie im Abschnitt dieses Themas unter [Anforderungen für gruppenverwaltete Dienstkonten](#).

Einführung

Wenn sich ein Clientcomputer mit einem auf einer Serverfarm gehosteten Dienst mithilfe des Netzwerklastenausgleichs (Network Load Balancing, NLB) oder einer anderen Methode verbindet, in der der Client alle Server als gleichen Dienst interpretiert, dann können die gegenseitige Authentifizierung unterstützende Authentifizierungsprotokolle wie Kerberos nicht verwendet werden, es sei denn, alle Instanzen der Dienste verwenden denselben Prinzipal. Das heißt, dass jeder Dienst dieselben Kennwörter/Schlüssel zum Beweisen der entsprechenden Identität verwenden muss.

NOTE

Failovercluster unterstützen keine gruppenverwalteten Dienstkonten. Dienste, die oben im Clusterdienst ausgeführt werden, können jedoch ein gMSA oder sMSA verwenden, wenn sie ein Windows-Dienst, ein App-Pool, eine geplante Aufgabe oder gMSA oder sMSA systemeigen unterstützen.

Dienste verfügen über die folgenden Prinzipale, aus denen ausgewählt werden kann, und jeder hat bestimmte Begrenzungen.

| PRINCIPALS | SCOPE | UNTERSTÜTZTE DIENSTE | KENNWORTVERWALTUNG |
|--|--------|---|---|
| Computerkonto von Windows-System | Domäne | Auf einen mit einer Domäne verbundenen Server | Vom Computer verwaltet |
| Computerkonto ohne Windows-System | Domäne | Jeder mit einer Domäne verbundene Server | Keine |
| Virtuelles Konto | Lokal | Auf einen Server begrenzt | Vom Computer verwaltet |
| Eigenständig verwaltetes Windows 7-Dienstkonto | Domäne | Auf einen mit einer Domäne verbundenen Server | Vom Computer verwaltet |
| Benutzerkonto | Domäne | Jeder mit einer Domäne verbundene Server | Keine |
| Gruppenverwaltetes Dienstkonto | Domäne | Alle in die Domäne eingebundenen Windows Server 2012-Server | Der Domänencontroller verwaltet, und der Host ruft ab |

Ein Windows-Computerkonto oder ein eigenständiges verwaltetes Windows 7-Dienstkonto (standalone Managed Service Account, sMSA) oder virtuelle Konten können nicht über mehrere Systeme hinweg freigegeben werden. Wenn Sie ein Konto für Dienste auf freizugebenden Serverfarmen konfigurieren, müssten Sie getrennt vom Windows-System ein Benutzer- oder Computerkonto auswählen. So oder so verfügen diese Konten nicht über die Fähigkeit der Kennwortverwaltung über einen einzigen Steuerungspunkt. Dies führt zu einem Problem, wobei jede Organisation eine teure Lösung erstellen muss, um die Schlüssel für den Dienst in Active Directory zu aktualisieren und anschließend die Schlüssel in allen Instanzen dieser Dienste bereitzustellen.

Mit Windows Server 2012 müssen Dienste oder Dienst Administratoren die Kenn Wort Synchronisierung zwischen Dienst Instanzen nicht verwalten, wenn Sie Gruppen verwaltete Dienst Konten (Group Managed Service Accounts, gMSA) verwenden. Sie stellen die gruppenverwalteten Dienstkonten in Active Directory bereit und konfigurieren anschließend den Dienst, der verwaltete Dienstkonten unterstützt. Sie können ein gruppenverwaltetes Dienstkonto mithilfe der Cmdlets „*-ADServiceAccount“ bereitstellen, die Bestandteil des Active Directory-Moduls sind. Die Dienstidentitätskonfiguration auf dem Host wird unterstützt durch:

- Dieselben APIs wie sMSA, sodass Produkte, die sMSA unterstützen, auch gMSA unterstützen
- Dienste, die den Dienststeuerungs-Manager zum Konfigurieren der Anmeldeidentität verwenden
- Dienste, die den IIS-Manager für Anwendungspools zwecks Konfiguration der Identität verwenden
- Aufgaben mithilfe der Aufgabenplanung.

Anforderungen für gruppenverwaltete Dienstkonten

Die folgende Tabelle führt die Betriebssystemanforderungen auf, damit die Kerberos-Authentifizierung mit Diensten mithilfe von gMSA funktioniert. Die Active Directory-Anforderungen sind im Anschluss an die Tabelle aufgeführt.

Zum Ausführen der Windows PowerShell-Befehle ist eine 64-Bit-Architektur erforderlich, die zum Verwalten von gruppenverwalteten Dienstkonten (group Managed Service Accounts, gMSA) verwendet werden.

Betriebssystemanforderungen

| ELEMENT | ANFORDERUNG | BETRIEBSSYSTEM |
|--------------------------|-------------------------------|-----------------------|
| Host der Clientanwendung | RFC-konformer Kerberos-Client | Mindestens Windows XP |

| ELEMENT | ANFORDERUNG | BETRIEBSSYSTEM |
|--|---|---|
| Domänen Controller der Domäne des Benutzerkontos | RFC-konformer KDC | Mindestens Windows Server 2003 |
| Mitgliederhosts für freigegebene Dienste | | Windows Server 2012 |
| Domänen DCS des Mitglieds Hosts | RFC-konformer KDC | Mindestens Windows Server 2003 |
| Domänen DCS des GMSA-Kontos | Windows Server 2012 DCS verfügbar für den Host zum Abrufen des Kennworts | Domäne mit Windows Server 2012, die einige Systeme vor Windows Server 2012 haben kann |
| Back-End-Diensthost | RFC-konformer Kerberos-Anwendungsserver | Mindestens Windows Server 2003 |
| Domänen Controller des Back-End-Dienst Kontos | RFC-konformer KDC | Mindestens Windows Server 2003 |
| Windows PowerShell für Active Directory | Die lokal auf einem Computer oder auf Ihrem Remoteverwaltungscomputer (beispielsweise mithilfe des Remoteserver-Verwaltungstoolkits) installierte Windows PowerShell für Active Directory, die eine 64-Bit-Architektur unterstützt. | Windows Server 2012 |

Anforderungen für Active Directory-Domänendienste

- Das Active Directory Schema in der Gesamtstruktur der GMSA-Domäne muss auf Windows Server 2012 aktualisiert werden, um ein GMSA zu erstellen.

Sie können das Schema aktualisieren, indem Sie einen Domänen Controller installieren, auf dem Windows Server 2012 ausgeführt wird, oder indem Sie die Version von "Adprep.exe" auf einem Computer mit Windows Server 2012 ausführen. Das Objektversionsattribut für das Objekt „CN=Schema,CN=Configuration,DC=Contoso,DC=Com“ muss „52“ sein.

- Neues gruppenverwaltetes Dienstkonto
- Wenn Sie die Diensthostberechtigung verwalten, um das gMSA nach Gruppe zu verwenden, dann neue oder vorhandene Sicherheitsgruppe
- Beim Verwalten der Dienstzugriffssteuerung nach Gruppe dann neue oder vorhandene Sicherheitsgruppe
- Wenn erste Hauptstammschlüssel für Active Directory nicht in der Domäne bereitgestellt wird oder nicht erstellt wurde, dann erstellen Sie ihn. Die Ergebnisse seiner Erstellung können im KdsSvc-Betriebsprotokoll unter Ereignis-ID 4004 nachvollzogen werden.

Anweisungen zum Erstellen des Schlüssels finden Sie unter [Erstellen des Schlüssel Verteilungs Dienste-KDS-Stamm Schlüssels](#). Der Microsoft-Schlüsselverteilungsdienst („kdssvc.dll“) ist der Stammschlüssel für Active Directory.

Lebens

Der Lebenszyklus einer Serverfarm, die das gMSA-Feature verwendet, umfasst für gewöhnlich folgende Aufgaben:

- Bereitstellen einer neuen Serverfarm

- Hinzufügen von Mitgliedshosts zu einer vorhandenen Serverfarm
- Außerbetriebsetzung von Mitgliedshosts in einer vorhandenen Serverfarm
- Außerbetriebsetzung einer vorhandenen Serverfarm
- Entfernen eines gefährdeten Mitgliedshosts aus einer Serverfarm, sofern erforderlich.

Bereitstellen einer neuen Serverfarm

Beim Bereitstellen einer neuen Serverfarm muss der Dienstadministrator Folgendes bestimmen:

- Ob der Dienst mithilfe von gMSAs unterstützt wird
- Ob für den Dienst eingehende oder ausgehende authentifizierte Verbindungen erforderlich sind
- Die Computerkontennamen für die Mitgliedshosts für den Dienst mithilfe des gMSAs
- Den NetBIOS-Namen für den Dienst
- Den DNS-Hostnamen für den Dienst
- Die Dienstprinzipalnamen für den Dienst
- Das Kennwortänderungsintervall (Standard liegt bei 30 Tagen)

Schritt 1: Bereitstellen gruppenverwalteter Dienstkonten

Sie können ein GMSA nur erstellen, wenn das Gesamtstruktur Schema auf Windows Server 2012 aktualisiert wurde, der Hauptstamm Schlüssel für Active Directory bereitgestellt wurde und mindestens ein Windows Server 2012 DC in der Domäne vorhanden ist, in der das GMSA erstellt wird.

Die Mitgliedschaft in **Domänen-Admins**, **Konten-Operatoren** oder Fähigkeit zum Erstellen von „msDS-GroupManagedServiceAccount“-Objekten ist die Mindestvoraussetzung, um die folgenden Verfahren abzuschließen.

NOTE

Ein Wert für den Parameter "-Name" ist immer erforderlich (unabhängig davon, ob Sie "-Name" angeben), mit "-dNSHostName", "-restricttosinglecomputer" und "-restricttooutboundauthentication" sind sekundäre Anforderungen für die drei Bereitstellungs Szenarien.

So erstellen Sie ein gMSA mithilfe des Cmdlets „New-ADServiceAccount“

1. Führen Sie auf dem Windows Server 2012-Domänen Controller Windows PowerShell über die Taskleiste aus.
2. Geben Sie an der Befehlszeile für die Windows PowerShell die folgenden Befehle ein, und drücken Sie die EINGABETASTE: (Das Active Directory-Modul wird automatisch geladen.)

```
New-ADServiceAccount [-Name] <String> -dNSHostName <String> [-kerberosencryptiontype <adkerberosencryptiontype>] [-managedpasswordintervalindays <NULL-Werte zulassen [Int32]>] [-principalsallowedtoretrievemanagedpassword <ADPrincipal []>] [-sAMAccountName <String>] [-ServicePrincipalNames <String []>]
```

| PARAMETER | STRING | BEISPIEL |
|-------------|--------------------------|---------------------|
| Name | Name des Kontos | ITFarm1 |
| DNSHostName | DNS-Hostname des Diensts | ITFarm1.contoso.com |

| PARAMETER | STRING | BEISPIEL |
|--|---|---|
| KerberosEncryptionType | Jeder durch die Hostserver unterstützte Verschlüsselungstyp | None, RC4, AES128, AES256 |
| ManagedPasswordIntervallInDays | Kennwortänderungsintervall in Tagen (Standard liegt bei 30, wenn keine Angabe erfolgt) | 90 |
| PrincipalsAllowedToRetrieveManagedPassword | Die Computerkonten des Mitgliedhosts oder der Sicherheitsgruppe, die das Mitglied hostet, sind Mitglied von | ITFarmHosts |
| SamAccountName | NetBIOS-Name für den Dienst, sofern dies nicht „Name“ entspricht | ITFarm1 |
| ServicePrincipalNames | Die Dienstprinzipalnamen für den Dienst | http/"itfarm1". "c#", "c", "" itfarm1 "..... com", "http/. c", "MSSQLSvc/" itfarm1 ". ", "MSSQLSvc/" itfarm1 ".... com", "MSSQLSvc/INST01. Configuration. com:" |

IMPORTANT

Das Kennwortänderungsintervall kann nur während der Erstellung festgelegt werden. Wenn Sie das Intervall ändern möchten, müssen Sie ein neues gMSA erstellen und es zur Erstellungszeit festlegen.

Beispiel

Geben Sie jeden Befehl in einer einzelnen Zeile ein, auch wenn es den Anschein hat, dass aufgrund von Formatierungseinschränkungen Zeilenumbrüche vorhanden sind.

```
New-ADServiceAccount ITFarm1 -DNSHostName ITFarm1.contoso.com -
PrincipalsAllowedToRetrieveManagedPassword ITFarmHosts$ -KerberosEncryptionType RC4, AES128, AES256 -
ServicePrincipalNames http/ITFarm1.contoso.com/contoso.com, http/ITFarm1.contoso.com/contoso,
http/ITFarm1/contoso.com, http/ITFarm1/contoso
```

Die Mitgliedschaft in **Domänen-Admins**, **Konten-Operatoren** oder Fähigkeit zum Erstellen von „msDS-GroupManagedServiceAccount“-Objekten ist die Mindestvoraussetzung, um dieses Verfahren abzuschließen. Detaillierte Informationen zu den geeigneten Konten und Gruppenmitgliedschaften finden Sie unter [Lokale und Domänenstandardgruppen](#).

So erstellen Sie ein gMSA ausschließlich für die ausgehende Authentifizierung mithilfe des Cmdlets „New-ADServiceAccount“

1. Führen Sie auf dem Windows Server 2012-Domänen Controller Windows PowerShell über die Taskleiste aus.
2. Geben Sie an der Befehlszeile für das Windows PowerShell Active Directory-Modul die folgenden Befehle ein, und drücken Sie auf die EINGABETASTE:

```
New-ADServiceAccount [-Name] <String> -restricttooutboundauthenticationonly [-
managedpasswordintervalindays <Nullable [Int32]>] [-
principalsallowedtoretrievemanagedpassword <ADPrincipal []>]
```

| PARAMETER | STRING | BEISPIEL |
|--|---|-------------|
| Name | Benennen Sie das Konto | ITFarm1 |
| ManagedPasswordIntervallInDays | Kennwortänderungsintervall in Tagen (Standard liegt bei 30, wenn keine Angabe erfolgt) | 75 |
| PrincipalsAllowedToRetrieveManagedPassword | Die Computerkonten des Mitgliedhosts oder der Sicherheitsgruppe, die das Mitglied hostet, sind Mitglied von | ITFarmHosts |

IMPORTANT

Das Kennwortänderungsintervall kann nur während der Erstellung festgelegt werden. Wenn Sie das Intervall ändern möchten, müssen Sie ein neues gMSA erstellen und es zur Erstellungszeit festlegen.

Beispiel

```
New-ADServiceAccount ITFarm1 -RestrictToOutboundAuthenticationOnly -
PrincipalsAllowedToRetrieveManagedPassword ITFarmHosts$
```

Schritt 2: Konfigurieren des Dienstidentitäts-Anwendungsdiensts

Informationen zum Konfigurieren der Dienste in Windows Server 2012 finden Sie in der folgenden Featuredokumentation:

- IIS-Anwendungspool

Weitere Informationen finden Sie unter [Angabe einer Identität für einen Anwendungspool \(IIS 7\)](#).

- Windows-Dienste

Weitere Informationen finden Sie unter [Dienste](#).

- Aufgaben

Weitere Informationen finden Sie unter [Aufgabenplanung \(Übersicht\)](#).

Andere Dienste könnten gMSA unterstützen. Konsultieren Sie die entsprechende Produktdokumentation, um Details darüber zu erhalten, wie diese Dienste zu konfigurieren sind.

Hinzufügen von Mitgliedshosts zu einer vorhandenen Serverfarm

Wenn Sie Sicherheitsgruppen für die Verwaltung von Mitglied Hosts verwenden, fügen Sie das Computer Konto für den neuen Mitglieds Host der Sicherheitsgruppe (die Mitglieder Hosts des GMSA angehören) mithilfe einer der folgenden Methoden hinzu.

Die Mitgliedschaft in **Domänen-Admins** oder die Fähigkeit, Mitglieder zum Sicherheitsgruppenobjekt hinzuzufügen, ist die Mindestvoraussetzung zum Abschließen dieser Verfahren.

- Methode 1: Active Directory-Benutzer und-Computer

Verfahren zum Verwenden dieser Methode mithilfe der Windows-Benutzeroberfläche finden Sie unter [Hinzufügen eines Computerkontos zu einer Gruppe](#) und [Verwalten unterschiedlicher Domänen im Active Directory-Verwaltungszentrum](#).

- Methode 2: „dsmod“

Verfahren zum Verwenden dieser Methode mithilfe der Befehlszeile finden Sie unter [Hinzufügen eines Computerkontos zu einer Gruppe](#).

- Methode 3: Windows PowerShell Active Directory-Cmdlet „Add-ADPrincipalGroupMembership“

Verfahren zum Verwenden dieser Methode finden Sie unter [Add-ADPrincipalGroupMembership](#).

Suchen Sie bei der Verwendung von Benutzerkonten nach vorhandenen Konten, und fügen Sie dann das neue Benutzerkonto hinzu.

Die Mitgliedschaft in **Domänen-Admins**, **Konten-Operatoren** oder Fähigkeit zum Verwalten von „msDS-GroupManagedServiceAccount“-Objekten ist die Mindestvoraussetzung, um dieses Verfahren abzuschließen. Detaillierte Informationen zu den geeigneten Konten und Gruppenmitgliedschaften finden Sie unter „Lokale und Domänenstandardgruppen“.

So fügen Sie Hosts mithilfe des Cmdlets „Set-ADServiceAccount“ hinzu

1. Führen Sie auf dem Windows Server 2012-Domänen Controller Windows PowerShell über die Taskleiste aus.
2. Geben Sie an der Befehlszeile für das Windows PowerShell Active Directory-Modul die folgenden Befehle ein, und drücken Sie auf die EINGABETASTE:

```
Get-ADServiceAccount [-Identity] <String> -Properties  
principalsallowedtoretestevmanagedpassword
```

3. Geben Sie an der Befehlszeile für das Windows PowerShell Active Directory-Modul die folgenden Befehle ein, und drücken Sie auf die EINGABETASTE:

```
Set-ADServiceAccount [-Identity] <String> -principalsallowedtoretrievemanagedpassword  
<ADPrincipal [] >
```

| PARAMETER | STRING | BEISPIEL |
|--|---|---------------------|
| Name | Benennen Sie das Konto | ITFarm1 |
| PrincipalsAllowedToRetrieveManagedPassword | Die Computerkonten des Mitgliedhosts oder der Sicherheitsgruppe, die das Mitglied hostet, sind Mitglied von | Host1, Host2, Host3 |

Beispiel

Geben Sie beispielsweise zum Hinzufügen von Mitgliedhosts die folgenden Befehle ein, und drücken Sie dann die EINGABETASTE.

```
Get-ADServiceAccount [-Identity] ITFarm1 -Properties PrincipalsAllowedToRetrieveManagedPassword
```

```
Set-ADServiceAccount [-Identity] ITFarm1 -PrincipalsAllowedToRetrieveManagedPassword Host1$,Host2$,Host3$
```

Aktualisieren der Eigenschaften für gruppenverwaltete Dienstkonten

Die Mitgliedschaft in **Domänen-Admins**, **Konten-Operatoren** oder Fähigkeit zum Schreiben in „msDS-GroupManagedServiceAccount“-Objekte ist die Mindestvoraussetzung, um diese Verfahren abzuschließen.

Öffnen Sie das Active Directory-Modul für die Windows PowerShell, und legen Sie eine beliebige Eigenschaft

mithilfe des Cmdlets „Set-ADServiceAccount“ fest.

Detaillierte Informationen für das Festlegen dieser Eigenschaften finden Sie unter [Set-ADServiceAccount](#) in der TechNet-Bibliothek, oder indem Sie an der Eingabeaufforderung für das Active Directory-Modul für Windows PowerShell **Get-Help Set-ADServiceAccount** eingeben und die EINGABETASTE drücken.

Außerbetriebsetzung von Mitgliedshosts in einer vorhandenen Serverfarm

Die Mitgliedschaft in **Domänen-Admins** oder die Fähigkeit, Mitglieder aus dem Sicherheitsgruppenobjekt zu entfernen, ist die Mindestvoraussetzung zum Abschließen dieser Verfahren.

Schritt 1: Entfernen von Mitgliedshosts vom GMSA

Wenn Sie Sicherheitsgruppen für die Verwaltung von Mitglieds Hosts verwenden, entfernen Sie das Computer Konto für den außer Betrieb gesetzten Mitglieds Host aus der Sicherheitsgruppe, der die Mitglieder Hosts des GMSA angehören. verwenden Sie dazu eine der folgenden Methoden.

- Methode 1: Active Directory-Benutzer und-Computer

Verfahren zum Verwenden dieser Methode mithilfe der Windows-Benutzeroberfläche finden Sie unter [Löschen eines Computerkontos](#) und [Verwalten unterschiedlicher Domänen im Active Directory-Verwaltungszentrum](#).

- Methode 2: „drsm“

Verfahren zum Verwenden dieser Methode mithilfe der Befehlszeile finden Sie unter [Löschen eines Computerkontos](#).

- Methode 3: Windows PowerShell Active Directory-Cmdlet „Remove-ADPrincipalGroupMembership“

Detaillierte Informationen dazu, wie Sie dies vornehmen können, finden Sie unter [Remove-ADPrincipalGroupMembership](#) in der TechNet-Bibliothek, oder indem Sie an der Eingabeaufforderung für das Active Directory-Modul für Windows PowerShell **Get-Help Remove-ADPrincipalGroupMembership** eingeben und die EINGABETASTE drücken.

Wenn Sie Computerkonten auflisten, rufen Sie die vorhandenen Konten ab, und fügen Sie dann alle mit Ausnahme des entfernten Computerkontos hinzu.

Die Mitgliedschaft in **Domänen-Admins**, **Konten-Operatoren** oder Fähigkeit zum Verwalten von „msDS-GroupManagedServiceAccount“-Objekten ist die Mindestvoraussetzung, um dieses Verfahren abzuschließen. Detaillierte Informationen zu den geeigneten Konten und Gruppenmitgliedschaften finden Sie unter „Lokale und Domänenstandardgruppen“.

So entfernen Sie Hosts mithilfe des Cmdlets „Set-ADServiceAccount“

1. Führen Sie auf dem Windows Server 2012-Domänen Controller Windows PowerShell über die Taskleiste aus.
2. Geben Sie an der Befehlszeile für das Windows PowerShell Active Directory-Modul die folgenden Befehle ein, und drücken Sie auf die EINGABETASTE:

```
Get-ADServiceAccount [-Identity] <String> -Properties  
principalsallowedtoretestevemanagedpassword
```

3. Geben Sie an der Befehlszeile für das Windows PowerShell Active Directory-Modul die folgenden Befehle ein, und drücken Sie auf die EINGABETASTE:

```
Set-ADServiceAccount [-Identity] <String> -principalsallowedtoretrievemanagedpassword  
<ADPrincipal [] >
```

| PARAMETER | STRING | BEISPIEL |
|--|---|--------------|
| Name | Benennen Sie das Konto | ITFarm1 |
| PrincipalsAllowedToRetrieveManagedPassword | Die Computerkonten des Mitgliedhosts oder der Sicherheitsgruppe, die das Mitglied hostet, sind Mitglied von | Host1, Host3 |

Beispiel

Geben Sie beispielsweise zum Entfernen von Mitgliedhosts die folgenden Befehle ein, und drücken Sie dann die EINGABETASTE.

```
Get-ADServiceAccount [-Identity] ITFarm1 -Properties PrincipalsAllowedToRetrieveManagedPassword
```

```
Set-ADServiceAccount [-Identity] ITFarm1 -PrincipalsAllowedToRetrieveManagedPassword Host1$,Host3$
```

Schritt 2: Entfernen eines gruppenverwalteten Dienstkontos aus dem System

Entfernen Sie die zwischengespeicherten gruppenverwalteten Dienstkonto-Anmeldeinformationen aus dem Mitgliedhost unter Verwendung der „Uninstall-ADServiceAccount“- oder der „NetRemoveServiceAccount“ auf dem Hostsystem.

Sie müssen mindestens Mitglied der Gruppe **Administratoren** oder einer entsprechenden Gruppe sein, um diese Verfahren abschließen zu können.

So entfernen Sie ein gruppenverwaltetes Dienstkonto mithilfe des Cmdlets „Uninstall-ADServiceAccount“

1. Führen Sie auf dem Windows Server 2012-Domänen Controller Windows PowerShell über die Taskleiste aus.
2. Geben Sie an der Befehlszeile für das Windows PowerShell Active Directory-Modul die folgenden Befehle ein, und drücken Sie auf die EINGABETASTE:

Deinstallation: ADServiceAccount < ADServiceAccount>

Beispiel

Geben Sie den folgenden Befehl ein, und drücken Sie die EINGABETASTE, um beispielsweise die zwischengespeicherten Anmeldeinformationen für ein gruppenverwaltetes Dienstkonto namens „ITFarm1“ zu entfernen:

```
Uninstall-ADServiceAccount ITFarm1
```

Geben Sie für weitere Informationen über das Cmdlet Uninstall-ADServiceAccount an der Eingabeaufforderung für das Active Directory-Modul für Windows PowerShell **Get-Help Uninstall-ADServiceAccount** ein, und drücken Sie dann die EINGABETASTE, oder konsultieren Sie die Informationen auf der TechNet-Website unter [Uninstall-ADServiceAccount](#).

Siehe auch

- [Group Managed Service Accounts Overview](#) (Übersicht über gruppenverwaltete Dienstkonten)

Erstellen des KDS-Stammschlüssels der Schlüsselverteilungsdienste

09.04.2020 • 4 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema für IT-Experten wird beschrieben, wie ein Microsoft-Schlüssel Verteilungsdienst-Stamm Schlüssel (kdssvc. dll) auf dem Domänen Controller mithilfe von Windows PowerShell zum Generieren von Kenn Wörtern für Gruppen verwaltete Dienst Konten in Windows Server 2012 oder höher erstellt wird.

Domänen Controller erfordern einen Stamm Schlüssel, um mit dem Erstellen von GMSA-Kenn Wörtern zu beginnen. Die Domänencontroller warten bis zu zehn Stunden ab der Erstellung, um allen Domänencontrollern zu ermöglichen, ihre AD-Replikation vor der Erstellung eines gMSA zu konvergieren. Bei den zehn Stunden handelt es sich um eine Sicherheitsmaßnahme, um zu verhindern, dass das Kennwort generiert wird, bevor alle Domänencontroller in der Umgebung in der Lage sind, auf gMSA-Anforderungen zu reagieren. Wenn Sie zu früh versuchen, ein GMSA zu verwenden, wurde der Schlüssel möglicherweise nicht auf allen Domänen Controllern repliziert. Daher kann das Abrufen des Kennworts fehlschlagen, wenn der GMSA-Host versucht, das Kennwort abzurufen. Fehler beim gMSA-Kennwortabruf können auch auftreten, wenn Domänencontroller mit begrenzten Replikationszeitplänen verwendet werden oder wenn ein Replikationsproblem auftritt.

NOTE

Das Löschen und erneute Erstellen des Stamm Schlüssels kann zu Problemen führen, bei denen der alte Schlüssel nach dem Löschen weiterhin verwendet wird, da der Schlüssel zwischengespeichert wird. Der Schlüssel Verteilungsdienst (Key Distribution Service, KDC) sollte auf allen Domänen Controllern neu gestartet werden, wenn der Stamm Schlüssel neu erstellt wird.

Sie müssen mindestens Mitglied der Gruppe **Domänen-Admins**, **Organisations-Admins** oder einer entsprechenden Gruppe sein, damit Sie dieses Verfahren ausführen können. Detaillierte Informationen zu den geeigneten Konten und Gruppenmitgliedschaften finden Sie unter [Lokale und Domänenstandardgruppen](#).

NOTE

Zum Ausführen der Windows PowerShell-Befehle ist eine 64-Bit-Architektur erforderlich, die zum Verwalten von gruppenverwalteten Dienstkonten (group Managed Service Accounts, gMSA) verwendet werden.

So erstellen Sie den KDS-Stamm Schlüssel mithilfe des Cmdlets "Add-kdsrootkey"

1. Führen Sie auf dem Domänen Controller Windows Server 2012 oder höher Windows PowerShell über die Taskleiste aus.
2. Geben Sie an der Befehlszeile für das Windows PowerShell Active Directory-Modul die folgenden Befehle ein, und drücken Sie die EINGABETASTE:

Add-kdsrootkey-effectiveimmediately

TIP

Der Parameter „Effective time“ kann verwendet werden, um Schlüsseln vor der Verwendung die Zeit zu geben, auf alle Domänencontroller aufgefüllt zu werden. Durch die Verwendung von "Add-kdsrootkey-effectiveimmediately" wird ein Stamm Schlüssel zum Zieldomänen Controller hinzugefügt, der sofort vom KDS-Dienst verwendet wird. Andere Domänen Controller können den Stamm Schlüssel jedoch erst verwenden, wenn die Replikation erfolgreich war.

Für Testumgebungen mit nur einem Domänencontroller können Sie einen KDS-Stammschlüssel erstellen und die Startzeit in der Vergangenheit festlegen, um zu vermeiden, dass das Intervall auf die Schlüsselgenerierung wartet, indem folgende Vorgehensweise verwendet wird. Überprüfen Sie, ob ein 4004-Ereignis im KDS-Ereignisprotokoll protokolliert wurde.

So erstellen Sie den KDS-Stammschlüssel in einer Testumgebung mit unmittelbarer Wirksamkeit

1. Führen Sie auf dem Domänen Controller Windows Server 2012 oder höher Windows PowerShell über die Taskleiste aus.
2. Geben Sie an der Befehlszeile für das Windows PowerShell Active Directory-Modul die folgenden Befehle ein, und drücken Sie die EINGABETASTE:

```
$a = Get-Date
```

```
$b = $a. AddHours (-10)
```

```
Add-kdsrootkey-effectivetime-$b
```

Oder verwenden Sie einen einzelnen Befehl:

```
Add-kdsrootkey-effectivetime ((Get-Date). AddHours (-10))
```

Weitere Informationen

[Erste Schritte mit gruppenverwalteten Dienstkonten](#)

Kerberos Authentication Overview

09.04.2020 • 5 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Kerberos ist ein Authentifizierungsprotokoll zur Überprüfung der Identität eines Benutzers oder Hosts. Dieses Thema enthält Informationen zur Kerberos-Authentifizierung in Windows Server 2012 und Windows 8.

Featurebeschreibung

Mit dem Betriebssystem Windows Server werden das Authentifizierungsprotokoll Kerberos, Version 5, sowie Erweiterungen für die Authentifizierung mit öffentlichen Schlüsseln, den Transport von Autorisierungsdaten und die Delegierung implementiert. Der Kerberos-Authentifizierungs Client wird als Security Support Provider (SSP-) implementiert, und der Zugriff darauf erfolgt über die Security Support Provider-Schnittstelle (SSPI-). Die anfängliche Benutzerauthentifizierung ist in das Winlogon--für einmaliges Anmelden integriert.

Die Kerberos-Schlüsselverteilungscenter (KDC-) ist in andere Windows Server-Sicherheitsdienste integriert, die auf dem Domänen Controller ausgeführt werden. Der KDC verwendet die Active Directory Domain Services Datenbank der Domäne als Sicherheits Konten Datenbank. AD DS ist für Kerberos-Standardimplementierungen innerhalb der Domäne oder Gesamtstruktur erforderlich.

Praktische Anwendungen

Die Vorteile der Verwendung von Kerberos für die auf Domänen-basierende Authentifizierung sind folgende:

- **Delegierte Authentifizierung.**

Dienste, die unter Windows-Betriebssystemen ausgeführt werden, können die Identität eines Client Computers annehmen, wenn Sie im Auftrag des Clients auf Ressourcen zugreifen. In vielen Fällen kann ein Dienst die Arbeit für den Client abschließen, indem er auf Ressourcen auf dem lokalen Computer zugreift. Wenn ein Clientcomputer sich beim Dienst authentifiziert, bieten das NTLM- und Kerberos-Protokoll die Autorisierungsinformationen, die ein Dienst benötigt, um lokal die Identität des Clientcomputers anzunehmen. Einige verteilte Anwendungen sind jedoch so konzipiert, dass ein Front-End-Dienst die Identität des Client Computers verwenden muss, wenn er eine Verbindung mit Back-End-Diensten auf anderen Computern herstellt. Die Kerberos-Authentifizierung unterstützt einen Delegierungsmechanismus, der es einem Dienst ermöglicht, im Auftrag seines Clients zu fungieren, wenn eine Verbindung mit anderen Diensten hergestellt wird.

- **Einmaliges Anmelden.**

Mithilfe der Kerberos-Authentifizierung innerhalb einer Domäne oder Gesamtstruktur kann ein Benutzer oder Dienst auf Ressourcen mit der Erlaubnis von Administratoren auf Ressourcen zugreifen, ohne dass mehrere Anforderungen von Anmeldeinformationen erfolgen. Nach der ersten Anmeldung bei der Domäne über die Windows-Anmeldung verwaltet Kerberos die Anmeldeinformationen in der gesamten Gesamtstruktur, wenn ein Zugriff auf Ressourcen versucht wird.

- **Interoper.**

Die Implementierung des Kerberos V5-Protokolls von Microsoft basiert auf Standards-Nachverfolgen der Spezifikationen, die für die Internet Engineering Task Force (IETF) empfohlen werden. Bei Windows-Betriebssystemen schafft das Kerberos-Protokoll daher die Grundlage für die Interoperabilität mit anderen Netzwerken, in denen das Kerberos-Protokoll für die Authentifizierung verwendet wird. Darüber hinaus

veröffentlicht Microsoft eine Windows-Protokolldokumentation zur Implementierung des Kerberos-Protokolls. Die Dokumentation enthält technische Anforderungen, Einschränkungen, Abhängigkeiten und Windows-bestimmtes Protokoll Verhalten für die Microsoft-Implementierung des Kerberos-Protokolls.

- **Effizientere Authentifizierung bei Servern.**

Vor Kerberos konnte die NTLM-Authentifizierung verwendet werden, bei der ein Anwendungsserver eine Verbindung mit einem Domänencontroller herstellen muss, um jeden einzelnen Clientcomputer oder Dienst zu authentifizieren. Mithilfe des Kerberos-Protokolls ersetzen die Pass-the--durch die Authentifizierung durch die Authentifizierung. Der Server muss nicht zu einem Domänen Controller (wechseln, es sei denn, er muss ein Berechtigungs Attribut Zertifikat (PAC-))überprüfen. Stattdessen kann der Server den Clientcomputer authentifizieren, indem er vom Client vorgelegte Anmeldeinformationen untersucht. Clientcomputer können Anmeldeinformationen für einen bestimmten Server einmal erhalten und diese Anmeldeinformationen dann während einer Netzwerkanmeldesitzung wiederverwenden.

- **Gegenseitige Authentifizierung.**

Mithilfe des Kerberos-Protokolls kann ein Teilnehmer an einem der beiden Enden einer Netzwerkverbindung überprüfen, ob der Teilnehmer am anderen Ende die Entität ist, die er zu sein vorgibt. NTLM ermöglicht Clients nicht, die Identität eines Servers zu überprüfen oder einem Server zu ermöglichen, die Identität eines anderen Servers zu überprüfen. Die NTLM-Authentifizierung wurde für eine Netzwerkumgebung konzipiert, in die Echtheit der Server unterstellt wird. Das Kerberos-Protokoll geht nicht von derartigen Annahmen aus.

Weitere Informationen

[Windows-Authentifizierung: Übersicht](#)

What's New in Kerberos Authentication

09.04.2020 • 5 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016 und Windows 10

KDC-Unterstützung für vertrauenswürdige Authentifizierung mit öffentlichem Schlüssel

Ab Windows Server 2016 unterstützen KDCs eine Zuordnung von öffentlichen Schlüsseln. Wenn der öffentliche Schlüssel für ein Konto bereitgestellt wird, unterstützt der KDC Kerberos PKINIT explizit mithilfe des Schlüssels. Da keine Zertifikat Validierung vorhanden ist, werden selbst signierte Zertifikate unterstützt, und die Authentifizierungsmechanismen werden nicht unterstützt.

Die Schlüssel Vertrauensstellung wird bevorzugt, wenn Sie für ein Konto unabhängig von der Einstellung "Einstellung für" "Einstellung" "von" Einstellung "

Kerberos-Client und KDC-Unterstützung für RFC 8070 PKINIT-Erweiterung

Ab Windows 10, Version 1607 und Windows Server 2016, versuchen die Kerberos-Clients, die [RFC 8070 PKINIT-Erweiterung](#) für Anmeldungen mit öffentlichem Schlüssel zu registrieren.

Ab Windows Server 2016 können KDCs die Erweiterung PKINIT-Aktualität unterstützen. Standardmäßig bieten KDCs keine PKINIT-Aktualität-Erweiterung. Um es zu aktivieren, verwenden Sie die neue KDC-Unterstützung für die administrative Vorlage für die administrative Vorlage für die PKINIT-Erweiterung für alle DCS in der Domäne. Bei der Konfiguration werden die folgenden Optionen unterstützt, wenn die Domäne Windows Server 2016-Domänen Funktionsebene (DFL) ist:

- **Deaktiviert:** der KDC bietet die PKINIT-Erweiterung nie an und akzeptiert gültige Authentifizierungsanforderungen, ohne auf Aktualität zu prüfen. Benutzer erhalten nie die neue Identität der öffentlichen Schlüssel Identität.
- **Unterstützt:** PKINIT-Erweiterungen werden auf Anforderung unterstützt. Kerberos-Clients, die sich erfolgreich bei der PKINIT-Erweiterung authentifizieren, erhalten die aktuelle SID der öffentlichen Schlüssel Identität.
- **Erforderlich:** PKINIT-Erweiterung ist für die erfolgreiche Authentifizierung erforderlich. Kerberos-Clients, die die PKINIT-Erweiterung nicht unterstützen, schlagen immer fehl, wenn Anmelde Informationen für öffentliche Schlüssel verwendet werden.

Unterstützung von in die Domäne eingebundenen Geräten für die Authentifizierung mit öffentlichem Schlüssel

Ab Windows 10, Version 1507 und Windows Server 2016, kann das Gerät mithilfe der Kerberos-Authentifizierung bei einem Windows Server 2016-DC mit dem öffentlichen Schlüssel authentifiziert werden, wenn ein in eine Domäne eingebundenes Gerät seinen gebundenen öffentlichen Schlüssel bei einem Windows Server 2016-Domänen Controller (DC) registrieren kann. Weitere Informationen finden Sie unter [Authentifizierung mit öffentlichem Schlüssel für den Domänen Beitritt](#).

Kerberos-Clients lassen IPv4- und IPv6-Adress Hostnamen in Dienst Prinzipal Namen (SPNs) zu.

Ab Windows 10, Version 1507 und Windows Server 2016, können Kerberos-Clients für die Unterstützung von IPv4- und IPv6-Hostnamen in SPNs konfiguriert werden.

Registrierungspfad:

Hklm\software\microsoft\windows\currentversion\policies\system\kerberos\parameters

Erstellen Sie einen tryipspn-Eintrag, um die Unterstützung für IP-Adress Hostnamen in SPNs zu konfigurieren. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in 1. Wenn diese Eigenschaft nicht konfiguriert ist, wird nicht versucht, die Hostnamen der IP-Adressen

Wenn der SPN in Active Directory registriert ist, ist die Authentifizierung mit Kerberos erfolgreich.

Weitere Informationen finden Sie im Dokument [Konfigurieren von Kerberos für IP-Adressen](#).

KDC-Unterstützung für die Zuordnung von Schlüssel Vertrauens Konten

Ab Windows Server 2016 haben Domänen Controller Unterstützung für die Zuordnung von Schlüssel vertrauenswürdigen Konten sowie für das Fall Back auf vorhandene AltSecId und den Benutzer Prinzipal Namen (User Principal Name, UPN) im San-Verhalten. Wenn "" für "\subjectaltname" auf festgelegt ist:

- 0: eine explizite Zuordnung ist erforderlich. Dann muss Folgendes vorhanden sein:
 - Schlüssel Vertrauensstellung (neu mit Windows Server 2016)
 - Explizitl
- 1: implizite Zuordnung ist zulässig (Standard):
 1. Wenn die Schlüssel Vertrauensstellung für das Konto konfiguriert ist, wird Sie für die Zuordnung verwendet (neu mit Windows Server 2016).
 2. Wenn kein UPN im San vorhanden ist, wird für die Zuordnung von "AltSecId" versucht.
 3. Wenn ein UPN im San vorhanden ist, wird ein UPN-Wert für die Zuordnung versucht.

Weitere Informationen

- [Kerberos-Authentifizierung \(Übersicht\)](#)

Public Key Authentication für Geräte in einer Domäne

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Windows 10

Kerberos hat die Unterstützung von in die Domäne eingebundenen Geräten zum Anmelden mit einem Zertifikat ab Windows Server 2012 und Windows 8 hinzugefügt. Diese Änderung ermöglicht Drittanbietern das Erstellen von Lösungen zum Bereitstellen und Initialisieren von Zertifikaten für in die Domäne eingebundenen Geräten, die für die Domänen Authentifizierung verwendet werden sollen.

Automatische Bereitstellung öffentlicher Schlüssel

Ab Windows 10, Version 1507 und Windows Server 2016, stellen in die Domäne eingebundene Geräte automatisch einen gebundenen öffentlichen Schlüssel für einen Windows Server 2016-Domänen Controller (DC) bereit. Nachdem ein Schlüssel bereitgestellt wurde, kann Windows die Authentifizierung mit öffentlichem Schlüssel für die Domäne verwenden.

Schlüsselgenerierung

Wenn auf dem Gerät Credential Guard ausgeführt wird, wird ein öffentliches/privates Schlüsselpaar erstellt, das durch Credential Guard geschützt wird.

Wenn Credential Guard nicht verfügbar ist und ein TPM ist, wird ein öffentliches/privates Schlüsselpaar durch das TPM geschützt.

Wenn keines von beiden verfügbar ist, wird kein Schlüsselpaar generiert, und das Gerät kann sich nur mit einem Kennwort authentifizieren.

Öffentlicher Schlüssel für das Bereitstellen des Computer Kontos

Wenn Windows gestartet wird, wird überprüft, ob ein öffentlicher Schlüssel für sein Computer Konto bereitgestellt wurde. Wenn dies nicht der Fall ist, wird ein gebundener öffentlicher Schlüssel generiert und mit einem DC mit Windows Server 2016 oder höher für sein Konto konfiguriert. Wenn alle Domänen Controller auf eine Unterebene festgelegt sind, wird kein Schlüssel bereitgestellt.

Konfigurieren des Geräts für die Verwendung des öffentlichen Schlüssels

Wenn das Gruppenrichtlinie festlegen der **Unterstützung für die Geräte Authentifizierung mithilfe des Zertifikats** auf **Force** festgelegt ist, muss das Gerät einen Domänen Controller finden, auf dem Windows Server 2016 oder höher ausgeführt wird, um sich zu authentifizieren. Die Einstellung befindet sich unter Administrative Vorlagen > System > Kerberos.

Konfigurieren des Geräts für die Verwendung von Kennwort

Wenn die Unterstützung der Gruppenrichtlinie Einstellung für **die Geräte Authentifizierung mithilfe des Zertifikats** deaktiviert ist, wird immer das Kennwort verwendet. Die Einstellung befindet sich unter Administrative Vorlagen > System > Kerberos.

In die Domäne eingebundener Geräte Authentifizierung mit öffentlichem Schlüssel

Wenn Windows über ein Zertifikat für das in die Domäne eingebundenen Gerät verfügt, wird Kerberos zuerst

mithilfe des Zertifikats und bei Wiederholungsversuchen mit Kennwort authentifiziert. Dadurch kann sich das Gerät gegenüber DCS authentifizieren.

Da die automatisch bereitgestellten öffentlichen Schlüssel über ein selbst signiertes Zertifikat verfügen, schlägt die Zertifikat Überprüfung auf Domänen Controllern fehl, die die Zuordnung von Schlüssel Vertrauens Konten nicht unterstützen. Standardmäßig wird von Windows die Authentifizierung mit dem Domänen Kennwort des Geräts erneut versucht.

Kerberos Constrained Delegation Overview

09.04.2020 • 10 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Übersichts Thema für IT-Experten werden neue Funktionen für die eingeschränkte Kerberos-Delegation in Windows Server 2012 R2 und Windows Server 2012 beschrieben.

Funktionsbeschreibung

Die eingeschränkte Kerberos-Delegation wurde in Windows Server 2003 eingeführt, um eine sicherere Form der Delegation bereitzustellen, die von Diensten verwendet werden kann. Wenn dieses Feature konfiguriert ist, beschränkt die eingeschränkte Delegation die Dienste, für die ein angegebener Server im Auftrag eines Benutzers agieren kann. Dies erfordert Domänenadministratorrechte zum Konfigurieren eines Domänenkontos für einen Dienst und beschränkt das Konto auf eine einzige Domäne. In den heutigen Unternehmen sind Front-End-Dienste nicht auf die Integration in Dienste in Ihrer Domäne beschränkt.

In früheren Betriebssystemversionen, in denen der Dienst vom Domänenadministrator konfiguriert wurde, konnte der Dienstadministrator nicht ohne Weiteres feststellen, welche an die Ressourcendienste delegierten Front-End-Dienste ihm gehörten. Und zudem stellte jeder Front-End-Dienst, der an einen Ressourcendienst delegieren konnte, einen potenziellen Angriffspunkt dar. Wurde ein zum Delegieren an Ressourcendienste konfigurierter Server, der einen Front-End-Dienst hostete, gefährdet, konnten auch die Ressourcendienste gefährdet werden.

In Windows Server 2012 R2 und Windows Server 2012 wurde die Möglichkeit zum Konfigurieren der eingeschränkten Delegation für den Dienst vom Domänen Administrator an den Dienst Administrator übertragen. Dadurch erhält der Back-End-Dienstadministrator die Möglichkeit, Front-End-Dienste zuzulassen oder abzulehnen.

Ausführliche Informationen zu der in Windows Server 2003 eingeführten eingeschränkten Delegation finden Sie unter [Kerberos-Protokollübergang und eingeschränkte Delegation](#).

Die Implementierung des Kerberos-Protokolls in Windows Server 2012 R2 und Windows Server 2012 umfasst Erweiterungen speziell für die eingeschränkte Delegation. Service-for-User-to-Proxy (S4U2Proxy) ermöglicht es einem Dienst, mithilfe seines Kerberos-Diensttickets für einen Benutzer ein Diensticket aus dem Schlüsselverteilungscenter (Key Distribution Center, KDC) für einen Back-End-Dienst abzurufen. Diese Erweiterungen ermöglichen die Konfiguration der eingeschränkten Delegation für das Konto des Back-End-Diensteanbieters, das sich in einer anderen Domäne befinden kann. Weitere Informationen zu diesen Erweiterungen finden Sie in der MSDN Library unter [\[MS-SFU\]: Kerberos-Protokoll Erweiterungen: Dienst für Benutzer und eingeschränkte Delegierungs Protokollspezifikation](#).

Praktische Anwendungen

Die eingeschränkte Delegation bietet Dienst Administratoren die Möglichkeit, Anwendungs Vertrauensstellungs Grenzen anzugeben und zu erzwingen, indem Sie den Bereich einschränken, in dem Anwendungsdienste im Auftrag eines Benutzers agieren können. Dienstadministratoren können konfigurieren, welche Front-End-Dienstkonten die Authentifizierung an ihre Back-End-Dienste delegieren können.

Durch die Unterstützung der Domänen übergreifenden eingeschränkten Delegation in Windows Server 2012 R2 und Windows Server 2012 können Front-End-Dienste wie Microsoft Internet Security and Acceleration (ISA) Server, Microsoft Forefront Threat Management Gateway, Microsoft Exchange Outlook Webzugriff (OWA) und Microsoft SharePoint Server für die Verwendung der eingeschränkten Delegation für die Authentifizierung bei Servern in anderen Domänen konfiguriert werden. So können domänenübergreifende Dienstlösungen mit einer

vorhandenen Kerberos-Infrastruktur unterstützt werden. Die eingeschränkte Kerberos-Delegierung kann von Domänenadministratoren oder Dienstadministratoren verwaltet werden.

Domänenübergreifende, ressourcenbasierte eingeschränkte Delegierung

Mithilfe der eingeschränkten Kerberos-Delegierung kann eine eingeschränkte Delegierung bereitgestellt werden, wenn sich der Front-End-Dienst und die Ressourcendienste nicht in der gleichen Domäne befinden. Dienstadministratoren können die neue Delegierung konfigurieren, indem sie die Domänenkonten der Front-End-Dienste angeben, die die Identität von Benutzern für die Kontoobjekte der Ressourcendienste annehmen können.

Welchen Nutzen bietet diese Änderung?

Durch die Unterstützung der domänenübergreifenden eingeschränkten Delegierung können Dienste so konfiguriert werden, dass sie für die Authentifizierung bei Servern in anderen Domänen anstelle der uneingeschränkten Delegierung die eingeschränkte Delegierung verwenden. So kann anhand einer vorhandenen Kerberos-Infrastruktur Authentifizierungsunterstützung für domänenübergreifende Dienstlösungen bereitgestellt werden, ohne Front-End-Diensten für die Delegierung an einen Dienst vertrauen zu müssen.

Dadurch wird auch die Entscheidung verlagert, ob ein Server der Quelle einer Delegierten Identität vom Domänen Administrator delegieren an den Ressourcen Besitzer vertrauen soll.

Worin bestehen die Unterschiede?

Eine Änderung im zugrunde liegenden Protokoll ermöglicht die domänenübergreifende eingeschränkte Delegierung. Die Implementierung des Kerberos-Protokolls in Windows Server 2012 R2 und Windows Server 2012 umfasst Erweiterungen des Dienstanbieter für das Benutzer-zu-Proxy-Protokoll (S4U2Proxy). Diese Erweiterungen des Kerberos-Protokolls ermöglichen es einem Dienst, mithilfe seines Kerberos-Diensttickets für einen Benutzer ein Diensticket aus dem Schlüsselverteilungscenter für einen Back-End-Dienst abzurufen.

Implementierungs Informationen zu diesen Erweiterungen finden Sie unter [\[MS-SFU\]: Kerberos-Protokoll Erweiterungen: Dienst für Benutzer und eingeschränkte Delegierungs Protokollspezifikation](#) in MSDN.

Weitere Informationen zur grundlegenden Nachrichtensequenz für die Kerberos-Delegierung mit einem weitergeleiteten Ticket-Granting Ticket (TGT) im Vergleich zu Service-for-User-Erweiterungen (S4U) finden Sie im Abschnitt [1.3.3 Übersicht über das Protokoll](#) in [\[MS-SFU\]: Kerberos-Protokollerweiterungen: Protokollspezifikation für Service-for-User und eingeschränkte Delegierung](#).

Sicherheitsauswirkungen der ressourcenbasierten eingeschränkten Delegierung

Die ressourcenbasierte eingeschränkte Delegierung legt die Kontrolle über die Delegierung an den Administrator, der die Ressource besitzt, auf die zugegriffen wird. Dies hängt von den Attributen des Ressourcen Dienstanbieter und nicht vom Dienst ab, der als vertrauenswürdig eingestuft wird. Daher kann die ressourcenbasierte eingeschränkte Delegierung nicht das "Trusted-to-Authenticate-for-Delegation"-Bit verwenden, das zuvor den Protokoll Übergang gesteuert hat. Der KDC lässt beim Durchführen einer ressourcenbasierten eingeschränkten Delegierung immer den Protokoll Übergang zu, als wäre das Bit festgelegt.

Da das KDC den Protokoll Übergang nicht einschränkt, wurden zwei neue Bekannte SIDs eingeführt, um diesem Steuerelement den Ressourcen Administrator zu übergeben. Diese SIDs ermitteln, ob der Protokoll Übergang erfolgt ist, und können mit standardmäßigen Zugriffs Steuerungs Listen verwendet werden, um den Zugriff nach Bedarf zu erteilen oder einzuschränken.

| SID | BESCHREIBUNG |
|-----|--------------|
|-----|--------------|

| SID | BESCHREIBUNG |
|--|---|
| AUTHENTICATION_AUTHORITY_ASSERTED_IDENTITY
S-1-18-1 | Eine SID, die bedeutet, dass die Identität des Clients durch eine Authentifizierungs Stelle bestätigt wird, die auf dem Nachweis des Besitzes von Client Anmelde Informationen basiert. |
| SERVICE_ASSERTED_IDENTITY
S-1-18-2 | Eine SID, die bedeutet, dass die Identität des Clients von einem Dienst bestätigt wird. |

Ein Back-End-Dienst kann Standard-ACL-Ausdrücke verwenden, um die Authentifizierung des Benutzers zu bestimmen.

Wie konfiguriere ich die ressourcenbasierte eingeschränkte Delegierung?

Verwenden Sie Windows PowerShell-Cmdlets, um einen Ressourcendienst zum Zulassen des Front-End-Dienstzugriffs im Auftrag von Benutzern zu konfigurieren.

- Zum Abrufen einer Liste von Prinzipale verwenden Sie die Cmdlets **Get-adcomputer**, **Get-ADServiceAccount** und **Get-ADUser** mit dem Parameter **principalsallowedtodelegatetoaccount** .
- Um den Ressourcen Dienst zu konfigurieren, verwenden Sie die Cmdlets **New-adcomputer**, **New-ADServiceAccount**, **New-ADUser**, **Set-adcomputer**, **Set-ADServiceAccount** und **Set-ADUser** mit dem **principalsallowedtodelegatetoaccount** -Parameter.

Software Anforderungen

Die ressourcenbasierte eingeschränkte Delegierung kann nur auf einem Domänen Controller unter Windows Server 2012 R2 und Windows Server 2012 konfiguriert werden, kann jedoch in einer Gesamtstruktur mit gemischtem Modus angewendet werden.

Sie müssen den folgenden Hotfix auf allen Domänen Controllern unter Windows Server 2012 in Benutzerkonto Domänen auf dem Verweispfad zwischen den Front-End-und Back-End-Domänen anwenden, die Betriebssysteme vor Windows Server ausführen: ressourcenbasierte eingeschränkte Delegierung KDC_ERR_POLICY Fehler in Umgebungen mit Windows Server 2008 R2-basierten Domänen Controllern (<https://support.microsoft.com/en-gb/help/2665790/resource-based-constrained-delegation-kdc-err-policy-failure-in-enviro>).

Verhindern, dass ein Kennwort, das geheime RC4-Schlüssel verwendet, von Kerberos geändert wird

09.04.2020 • 4 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2008 R2 und Windows Server 2008

In diesem Thema für IT-Experten werden einige Einschränkungen im Kerberos-Protokoll erläutert, die dazu führen können, dass böswillige Benutzer die Kontrolle über das Konto eines Benutzers nehmen. Der Kerberos-Netzwerk Authentifizierungsdienst (V5) (RFC 4120), der in der Branche gut bekannt ist, gibt eine Einschränkung, bei der sich ein Angreifer als Benutzer authentifizieren oder das Kennwort des Benutzers ändern kann, wenn der Angreifer den geheimen Schlüssel des Benutzers kennt.

Der Besitz der von Kenn Wörtern abgeleiteten Kerberos-Schlüssel eines Benutzers (RC4 und Advanced Encryption Standard [AES]) wird standardmäßig bei der Kerberos-Kenn Wort Änderungs Änderung pro RFC 4757 überprüft. Das nur-Text-Kennwort des Benutzers wird niemals für den Schlüsselverteilungscenter (KDC) bereitgestellt, und Active Directory Domänen Controller besitzen standardmäßig keine Kopie von nur-Text-Kenn Wörtern für Konten. Wenn der Domänen Controller keinen Kerberos-Verschlüsselungstyp unterstützt, kann der geheime Schlüssel nicht zum Ändern des Kennworts verwendet werden.

In den Windows-Betriebssystemen, die in der Liste gilt für am Anfang dieses Themas angegeben sind, gibt es drei Möglichkeiten, um die Möglichkeit zum Ändern von Kenn Wörtern mithilfe von Kerberos mit RC4-geheimen Schlüsseln zu blockieren:

- Konfigurieren Sie das Benutzerkonto für die Konto Option Smartcard ist für die interaktive Anmeldung erforderlich. Dadurch wird der Benutzer darauf beschränkt, sich nur mit einer gültigen Smartcard anzumelden, damit RC4-Authentifizierungsdienst Anforderungen (as-reqs) abgelehnt werden. Klicken Sie mit der rechten Maustaste auf das Konto, klicken Sie auf Eigenschaften, und klicken Sie auf die Registerkarte Konto, um die Konto Optionen für ein Konto festzulegen.
- Deaktivieren Sie die RC4-Unterstützung für Kerberos auf allen Domänen Controllern. Dies erfordert mindestens eine Windows Server 2008-Domänen Funktionsebene und eine Umgebung, in der alle Kerberos-Clients, Anwendungsserver und Vertrauens Stellungen von und von der Domäne AES unterstützen müssen. Die Unterstützung für AES wurde in Windows Server 2008 und Windows Vista eingeführt.

[!NOTE] Es gibt ein bekanntes Problem beim Deaktivieren von RC4, das dazu führen kann, dass das System neu gestartet wird. Weitere Informationen finden Sie in den folgenden Hotfixes:

- [Windows Server 2012 R2](#)
- [Windows Server 2012](#)
- Für frühere Versionen von Windows Server ist kein Hotfix verfügbar.
- Stellen Sie Domänen auf Windows Server 2012 R2-Domänen Funktionsebene oder höher bereit, und konfigurieren Sie die Benutzer als Mitglieder der Sicherheitsgruppe "geschützte Benutzer". Da dieses Feature mehr als nur die RC4-Verwendung im Kerberos-Protokoll unterbricht, finden Sie weitere Informationen unter Ressourcen [im folgenden Abschnitt](#).

Weitere Informationen

- Informationen dazu, wie Sie die Verwendung des RC4-Verschlüsselungs Typs in Windows Server 2012 R2-Domänen verhindern, finden Sie unter [Sicherheitsgruppe "geschützte Benutzer"](#) und [Konfigurieren](#)

[geschützter Konten](#).

- Erläuterungen zu RFC 4120 und RFC 4757 finden Sie unter [IETF Documents \(IETF-Dokumente\)](#).

Kerberos-Clients lassen IPv4-und IPv6-Adress Hostnamen in Dienst Prinzipal Namen (SPNs) zu.

02.12.2019 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016

Ab Windows 10, Version 1507 und Windows Server 2016, können Kerberos-Clients für die Unterstützung von IPv4-und IPv6-Hostnamen in SPNs konfiguriert werden.

Standardmäßig versucht Windows nicht, die Kerberos-Authentifizierung für einen Host durchführen, wenn der Hostname eine IP-Adresse ist. Es wird auf andere aktivierte Authentifizierungsprotokolle wie NTLM zurückgegriffen. Anwendungen sind jedoch manchmal hart codiert, um IP-Adressen zu verwenden. Dies bedeutet, dass die Anwendung auf NTLM zurückgreift und nicht Kerberos verwendet. Dies kann zu Kompatibilitätsproblemen führen, wenn Umgebungen zum Deaktivieren von NTLM verschoben werden.

Um die Auswirkung der Deaktivierung von NTLM zu reduzieren, wurde eine neue Funktion eingeführt, die es Administratoren ermöglicht, IP-Adressen als Hostnamen in Dienst Prinzipal Namen zu verwenden. Diese Funktion wird auf dem Client über einen Registrierungsschlüssel Wert aktiviert.

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters" /v TryIPSPN /t REG_DWORD /d 1 /f
```

Erstellen Sie einen tryipspn-Eintrag, um die Unterstützung für IP-Adress Hostnamen in SPNs zu konfigurieren. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in 1. Dieser Registrierungs Wert muss auf jedem Client Computer festgelegt werden, der über die IP-Adresse auf durch Kerberos geschützte Ressourcen zugreifen muss.

Konfigurieren eines Dienst Prinzipal namens als IP-Adresse

Ein Dienst Prinzipal Name ist ein eindeutiger Bezeichner, der während der Kerberos-Authentifizierung zum Identifizieren eines Dienstanbieter verwendet wird. Ein SPN besteht aus einem Dienst, einem Hostnamen und optional einem Port in Form von `service/hostname[:port]`, wie `host/fs.contoso.com` z. b. Windows registriert mehrere SPNs bei einem Computer Objekt, wenn ein Computer mit Active Directory verknüpft ist.

IP-Adressen werden normalerweise nicht anstelle von Hostnamen verwendet, da IP-Adressen häufig temporär sind. Dies kann zu Konflikten und Authentifizierungs Fehlern führen, wenn Adressleases ablaufen und erneuert werden. Daher ist die Registrierung eines auf IP-Adressen basierenden SPN ein manueller Prozess und sollte nur verwendet werden, wenn es unmöglich ist, zu einem DNS-basierten Hostnamen zu wechseln.

Die empfohlene Vorgehensweise ist die Verwendung des Tools [Setspn.exe](#). Beachten Sie, dass ein SPN nur für ein einzelnes Konto in Active Directory registriert werden kann, daher wird empfohlen, dass IP-Adressen bei Verwendung von DHCP statische Leases aufweisen.

```
Setspn -s <service>/ip.address <domain-user-account>
```

Beispiel:

```
Setspn -s host/192.168.1.1 server01
```

NTLM: Übersicht

09.04.2020 • 5 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema für IT-Experten werden NTLM, alle Änderungen an der Funktionalität beschrieben und Links zu technischen Ressourcen für die Windows-Authentifizierung und NTLM für Windows Server 2012 und frühere Versionen bereitstellt.

Featurebeschreibung

Die NTLM-Authentifizierung ist eine Familie von Authentifizierungs Protokollen, die in der Windows Msv1_0.dll enthalten sind. Zu den NTLM-Authentifizierungsprotokollen gehören LAN-Manager Version 1 und 2 sowie NTLM Version 1 und 2. Die NTLM-Authentifizierungsprotokolle authentifizieren Benutzer und Computer basierend auf einer Herausforderung/Response-Mechanismus, der einem Server oder einem Domänen Controller bestätigt, dass ein Benutzer das mit einem Konto verknüpfte Kennwort kennt. Bei Verwendung des NTLM-Protokolls muss ein Ressourcenserver eine der folgenden Aktionen ausführen, um die Identität eines Computers oder Benutzers zu überprüfen, wenn ein neues Zugriffstoken benötigt wird:

- Kontaktieren eines Domänenauthentifizierungsdienstes auf dem Domänencontroller für die Kontodomäne des Computers oder Benutzers, wenn es sich um ein Domänenkonto handelt.
- Nachschlagen des Computer- oder Benutzerkontos in der lokalen Kontendatenbank, wenn es sich um ein lokales Konto handelt.

Aktuelle Anwendungen

Die NTLM-Authentifizierung wird weiterhin unterstützt und muss für die Windows-Authentifizierung bei Systemen verwendet werden, die als Mitglied einer Arbeitsgruppe konfiguriert sind. Die NTLM-Authentifizierung wird auch für die lokale Anmelde Authentifizierung auf nicht-Domänen Controllern verwendet. Die Kerberos-Authentifizierung (Version 5) ist die bevorzugte Authentifizierungsmethode für Active Directory Umgebungen, aber eine nicht-Microsoft-oder Microsoft-Anwendung verwendet möglicherweise weiterhin NTLM.

Die Verwendung des NTLM-Protokolls in einer IT-Umgebung zu reduzieren, setzt sowohl Kenntnisse der für NTLM geltenden Anwendungsanforderungen als auch der Strategien und Schritte voraus, die erforderlich sind, um Computerumgebungen für die Verwendung anderer Protokolle zu konfigurieren. Neue Tools und Einstellungen helfen Ihnen, zu entdecken, wie NTLM verwendet wird, um den NTLM-Verkehr selektiv einzuschränken. Informationen dazu, wie Sie die Verwendung von NTLM in Ihren Umgebungen analysieren und einschränken, finden Sie unter [Einführung der Einschränkung der NTLM-Authentifizierung](#), wo Sie auf Anleitungen zum Überwachen und Einschränken der Verwendung von NTLM zugreifen können.

Neue und geänderte Funktionalität

Es gibt keine Funktionsänderungen für NTLM für Windows Server 2012.

Entfernte oder veraltete Funktionen

Für NTLM für Windows Server 2012 gibt es keine entfernten oder veralteten Funktionen.

Server-Manager Informationen

NTLM kann nicht über den Server-Manager konfiguriert werden. Sie können Sicherheitsrichtlinieneinstellungen oder Gruppenrichtlinien verwenden, um die Verwendung der NTLM-Authentifizierung zwischen Computersystemen zu verwalten. In einer Domäne ist Kerberos das Standardauthentifizierungsprotokoll.

Siehe auch

In der folgenden Tabelle sind relevante Ressourcen für NTLM und andere Windows-Authentifizierungstechnologien aufgeführt.

| ART DES INHALTS | VERWEISE |
|---------------------|--|
| Produktbewertung | Einführung der Einschränkung der NTLM-Authentifizierung
Änderungen bei der NTLM-Authentifizierung |
| Planung | Leitfaden zur Bedrohungsmodellierung
Bedrohungen und Gegenmaßnahmen: Sicherheitseinstellungen in Windows Server 2003 und Windows XP
Leitfaden zu Bedrohungen und Gegenmaßnahmen: Sicherheitseinstellungen in Windows Server 2008 und Windows Vista
Leitfaden zu Bedrohungen und Gegenmaßnahmen: Sicherheitseinstellungen in Windows Server 2008 R2 und Windows 7 |
| Bereitstellung | Erweiterter Schutz für die Authentifizierung
Leitfaden zur Überwachung und Einschränkung der NTLM-Verwendung
Fragen Sie das Verzeichnisdienst Team: NTLM-Blockierung und Sie: Anwendungs Analyse-und-Überwachungsmethoden in Windows 7
Blog zur Windows-Authentifizierung
Konfigurieren von "MaxConcurrentApi" für NTLM-Pass-durch Authentifizierung |
| Entwickelt | Microsoft NTLM-(Windows)
[MS-nlmp]: NT LAN Manager (NTLM) Authentication Protocol Specification
[MS-NNTP]: NT-LAN-Manager (NTLM) Authentifizierung: Network News Transfer Protocol (NNTP-) Erweiterung
[MS-ntht]: NTLM over HTTP-Protokollspezifikation |
| Problembehandlung | Noch nicht verfügbar |
| Communityressourcen | Ist das Pferd noch tot: NTLM-Engpässe und die RPC-Laufzeit |

Kennwörter: Übersicht

09.04.2020 • 4 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema für IT-Experten werden Kenn Wörter beschrieben, die in den Windows-Betriebssystemen verwendet werden, sowie Links zu Dokumentationen und Diskussionen über die Verwendung von Kenn Wörtern in einer Strategie zur Verwaltung von Anmelde Informationen.

Featurebeschreibung

Betriebssysteme und Anwendungen sind heute mit Kenn Wörtern entworfen, und auch wenn Sie Smartcards oder biometrische Systeme verwenden, haben alle Konten weiterhin Kenn Wörter und können in einigen Fällen weiterhin verwendet werden. Einige Konten, insbesondere Konten, die zum Ausführen von Diensten verwendet werden, können nicht einmal Smartcards und biometrische Token verwenden und müssen daher ein Kennwort für die Authentifizierung verwenden. Windows schützt Kenn Wörter mithilfe kryptografischer Hashes.

Weitere Informationen zu Windows-Kenn Wörtern finden Sie unter [Technische Übersicht](#) über Kenn Wörter.

Praktische Anwendungen

In Windows und vielen anderen Betriebssystemen ist die häufigste Methode zum Authentifizieren der Identität eines Benutzers die Verwendung einer geheimen Passphrase oder eines geheimen Kennworts. Zum Sichern Ihrer Netzwerkumgebung müssen von allen Benutzern sichere Kenn Wörter verwendet werden. Dadurch wird verhindert, dass böswillige Benutzer ein schwaches Kennwort erraten, ob durch manuelle Methoden oder mithilfe von Tools, um die Anmelde Informationen eines kompromittierten Benutzerkontos zu erhalten. Dies gilt insbesondere für Administrator Konten. Wenn Sie ein komplexes Kennwort regelmäßig ändern, verringert es die Wahrscheinlichkeit, dass ein Kenn Wort Angriff dieses Konto kompromittiert.

Neue und geänderte Funktionalität

In Windows Server 2012 und Windows 8 sind Bild Kennwörter neu. Bild Kennwörter sind eine Kombination aus einem vom Benutzer ausgewählten Bild, das mit einer Reihe von Gesten verknüpft ist. Die Bild Kenn Wort Funktionalität ist auf Domänen-Computern deaktiviert. Links zu weiteren Informationen zu Bild Kennwörtern finden Sie unter [Siehe auch](#) weiter unten.

Die Kenn Wort Funktionalität in Windows Server 2012 und Windows 8 wurde nicht geändert. Es wurden keine neuen Gruppenrichtlinie Einstellungen hinzugefügt. Es wurden jedoch Verbesserungen und Verbesserungen an den Anmelde Informationen (und der Kenn Wort) Verwaltung vorgenommen, wie z. b. mit Bild Kennwörtern, locker für Anmelde Informationen und Anmelden bei Windows 8 mit einem Microsoft-Konto, früher als Windows Live ID bezeichnet.

Veraltete Funktionen

In Windows Server 2012 und Windows 8 wurden keine Kenn Wort Funktionen als veraltet markiert.

Software Anforderungen

In Unternehmensumgebungen werden Kenn Wörter in der Regel mit Active Directory Domain Services verwaltet. Kenn Wörter können auch auf dem lokalen Computer mit den Einstellungen unter Lokale Sicherheitseinstellungen,

Konto Richtlinien, Kenn Wort Richtlinie verwaltet werden.

Siehe auch

In dieser Tabelle werden zusätzliche Ressourcen für Kenn Wort Features, die Technologie und die Verwaltung von Anmelde Informationen aufgelistet.

| ART DES INHALTS | VERWEISE |
|-------------------------|--|
| Szenariodokumentation | Schutz Ihrer digitalen Identität |
| Betrieb | Active Directory von Benutzern und Computern |
| Problembehandlung | Ermitteln, wann Ihr Kennwort abläuft - Active Directory PowerShell-Blog |
| Sicherheit | Leitfaden zu Bedrohungen und Gegenmaßnahmen für Windows Server 2008 R2 und Windows 7: Konto Richtlinien
Leitfaden zum ändern und erstellen sicherer Kenn Wörter |
| Tools und Einstellungen | Referenz zu Gruppenrichtlinie Einstellungen für Windows und Windows Server im Microsoft Download Center |
| Communityressourcen | Schutz Ihrer digitalen Identität
Anmelden bei Windows 8 mit einer Windows Live ID
Anmelden mit einem Bild Kennwort
Optimieren der Bild Kenn Wort Sicherheit |

Übersicht über TLS/SSL (SChannel SSP)

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows 10

In diesem Thema für IT-Experten werden die TLS- und SSL-Implementierungen in Windows mithilfe des SChannel Security Service Provider (SSP) vorgestellt, indem praktische Anwendungen, Änderungen in der Implementierung von Microsoft und Softwareanforderungen sowie zusätzliche Ressourcen für Windows Server 2012 und Windows 8 beschrieben werden.

Beschreibung

SChannel ist ein Sicherheitsdiensteanbieter (Security Support Provider, SSP), der die Internet-Standardauthentifizierungsprotokolle SSL (Secure Sockets Layer) und TLS (Transport Layer Security) implementiert.

Die Security Support Provider-Schnittstelle (Security Support Provider Interface, SSPI) ist eine API, die von Windows-Systemen verwendet wird, um sicherheitsbezogene Funktionen wie Authentifizierungen durchzuführen. Die SSPI fungiert als gemeinsame Schnittstelle für mehrere SSPs, einschließlich des SChannel SSP.

Die TLS-Versionen 1,0, 1,1 und 1,2, die SSL-Versionen 2,0 und 3,0 sowie das Datagramm Transport Layer Security (DTLS) Protokollversion 1,0 und der Transport (PCT) des privaten Kommunikations Transports basieren auf der Kryptografie mit öffentlichem Schlüssel. Die SChannel-Authentifizierungsprotokollsammlung enthält diese Protokolle. Alle SChannel-Protokolle verwenden ein Client/Server-Modell.

Bereich

Ein Problem beim Verwalten eines Netzwerks ist das Sichern von Daten, die zwischen Anwendungen in einem nicht vertrauenswürdigen Netzwerk gesendet werden. Sie können TLS und SSL zum Authentifizieren von Servern und Client Computern verwenden und dann das Protokoll verwenden, um Nachrichten zwischen den authentifizierten Parteien zu verschlüsseln.

Sie können TLS/SSL beispielsweise für Folgendes verwenden:

- SSL-gesicherte Transaktionen mit einer E-Commerce-Website
- Authentifizierten Clientzugriff auf einer SSL-gesicherten Website
- Remotezugriff
- SQL-Zugriff
- E-Mail

Bedingungen

TLS- und SSL-Protokolle verwenden ein Client/Server-Modell und basieren auf der Zertifikat Authentifizierung, die eine Public Key-Infrastruktur erfordert.

Server-Manager Informationen

Zum Implementieren von TLS, SSL oder SChannel sind keine Konfigurationsschritte erforderlich.

Siehe auch

- Das SChannel-Sicherheitspaket
- Sicherer Kanal
- Transport Layer Security-Protokoll

TLS-Änderungen (Schannel SSP) in Windows 10 und Windows Server 2016

09.04.2020 • 10 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016 und Windows 10

Verschlüsselungs Sammlungs Änderungen

Windows 10, Version 1511 und Windows Server 2016 fügen Unterstützung für die Konfiguration der Verschlüsselung der Verschlüsselungs Suite mithilfe der Verwaltung mobiler Geräte (Mobile Device Management, MDM) hinzu.

Informationen zu den Änderungen der Prioritäts Reihenfolge der Verschlüsselungs Suite finden Sie unter Verschlüsselungs Sammlungen [in Schannel](#).

Unterstützung für die folgenden Verschlüsselungs Sammlungen hinzugefügt:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (RFC 5289) in Windows 10, Version 1507 und Windows Server 2016
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (RFC 5289) in Windows 10, Version 1507 und Windows Server 2016

Disabledbydefault-Änderung für die folgenden Verschlüsselungs Sammlungen:

- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (RFC 5246) in Windows 10, Version 1703
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (RFC 5246) in Windows 10, Version 1703
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA (RFC 5246) in Windows 10, Version 1703
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA (RFC 5246) in Windows 10, Version 1703
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (RFC 5246) in Windows 10, Version 1703
- TLS_RSA_WITH_RC4_128_SHA in Windows 10, Version 1709
- TLS_RSA_WITH_RC4_128_MD5 in Windows 10, Version 1709

Ab Windows 10, Version 1507 und Windows Server 2016, werden SHA 512-Zertifikate standardmäßig unterstützt.

RSA-Schlüssel Änderungen

Windows 10, Version 1507 und Windows Server 2016 fügen Sie Registrierungs Konfigurationsoptionen für Client-RSA-Schlüsselgrößen hinzu.

Weitere Informationen finden Sie unter [keyexchangealgorithmus-Client RSA Key sizes](#).

Diffie-Hellman-Schlüssel Änderungen

Windows 10, Version 1507 und Windows Server 2016 fügen Sie Registrierungs Konfigurationsoptionen für Diffie-Hellman-Schlüsselgrößen hinzu.

Weitere Informationen finden Sie unter [keyexchangealgorithmus-Diffie-Hellman-Schlüsselgrößen](#).

SCH_USE_STRONG_CRYPTO Option "Änderungen"

Mit Windows 10, Version 1507 und Windows Server 2016, deaktiviert [SCH_USE_STRONG_CRYPTO](#) Option jetzt NULL-, MD5-, des-und Export Chiffren.

Änderungen der elliptischen Kurve

Windows 10, Version 1507 und Windows Server 2016 fügen Gruppenrichtlinie Konfiguration für elliptische Kurven unter Computer Konfiguration > Administrative Vorlagen > Netzwerk > ssl-Konfigurationseinstellungen hinzu. Die ECC-Kurven Reihenfolge gibt die Reihenfolge an, in der elliptische Kurven bevorzugt werden, und ermöglicht unterstützte Kurven, die nicht aktiviert sind.

Unterstützung für die folgenden Ellipsen Kurven hinzugefügt:

- Benannte brainpoolp256r1 (RFC 7027) in Windows 10, Version 1507 und Windows Server 2016
- Benannte brainpoolp384r1 (RFC 7027) in Windows 10, Version 1507 und Windows Server 2016
- Benannte brainpoolp512r1 (RFC 7027) in Windows 10, Version 1507 und Windows Server 2016
- Curve25519 (RFC Draft-IETF-TLS-Curve25519) in Windows 10, Version 1607 und Windows Server 2016

Unterstützung für die Dispatch-Ebene für die versiesagemessage-&

Windows 10, Version 1507 und Windows Server 2016 fügen Unterstützung für "versiesagemessage/unversiesagemessage" auf dispatchebene hinzu.

DTLS 1,2

Windows 10, Version 1607 und Windows Server 2016, Unterstützung für DTLS 1,2 (RFC 6347) hinzufügen.

HTTP. SYS-Thread Pool

Windows 10, Version 1607 und Windows Server 2016 fügen Sie die Registrierungs Konfiguration der Größe des Thread Pools hinzu, der zum Verarbeiten von TLS-Handshakes für HTTP verwendet wird. Einsetzt.

Registrierungspfad:

HKLM\System\CurrentControlSet\Control\LSA

Um eine maximale Thread Pool Größe pro CPU-Kern anzugeben, erstellen Sie einen **maxasyncworkerthreadspercpu** -Eintrag. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in die gewünschte Größe. Wenn nicht konfiguriert, beträgt der Höchstwert 2 Threads pro CPU-Kern.

Unterstützung der nächsten Protokoll Aushandlung (NPN)

Ab Windows 10, Version 1703, wurde die nächste Protokoll Verhandlung (NPN) entfernt und wird nicht mehr unterstützt.

Vorinstallierter Schlüssel (PSK)

Windows 10, Version 1607 und Windows Server 2016 fügen Unterstützung für den PSK-Schlüsselaustausch Algorithmus (RFC 4279) hinzu.

Unterstützung für die folgenden PSK-Verschlüsselungen Sammlungen hinzugefügt:

- TLS_PSK_WITH_AES_128_CBC_SHA256 (RFC 5487) in Windows 10, Version 1607 und Windows Server 2016
- TLS_PSK_WITH_AES_256_CBC_SHA384 (RFC 5487) in Windows 10, Version 1607 und Windows Server 2016
- TLS_PSK_WITH_NULL_SHA256 (RFC 5487) in Windows 10, Version 1607 und Windows Server 2016
- TLS_PSK_WITH_NULL_SHA384 (RFC 5487) in Windows 10, Version 1607 und Windows Server 2016
- TLS_PSK_WITH_AES_128_GCM_SHA256 (RFC 5487) in Windows 10, Version 1607 und Windows Server 2016
- TLS_PSK_WITH_AES_256_GCM_SHA384 (RFC 5487) in Windows 10, Version 1607 und Windows Server 2016

Sitzungs Wiederaufnahme ohne serverseitige Verbesserung der serverseitigen Leistung

Windows 10, Version 1507 und Windows Server 2016 bieten im Vergleich zu Windows Server 2012 30% mehr Sitzungsfortläufe pro Sekunde mit Sitzungs Tickets.

Sitzungs Hash und erweiterte Erweiterung für den geheimen Hauptschlüssel

Windows 10, Version 1507 und Windows Server 2016 fügen Unterstützung für den RFC 7627: Transport Layer Security (TLS)-Sitzungs Hash und die erweiterte Erweiterung für den geheimen Hauptschlüssel hinzu.

Aufgrund dieser Änderung sind für Windows 10 und Windows Server 2016 Updates von Drittanbieter- [SSL-Anbietern](#) erforderlich, um NCrypt_Ssl_Interface_Version_3 zu unterstützen und diese neue Schnittstelle zu beschreiben.

SSL-Unterstützung

Ab Windows 10, Version 1607 und Windows Server 2016, sind der TLS-Client und der Server-SSL 3,0 standardmäßig deaktiviert. Dies bedeutet, dass der Client nicht SSL 3,0 anbietet oder akzeptiert, es sei denn, die Anwendung oder der Dienst fordert SSL 3,0 über die SSPI an, und der Server wählt niemals SSL 3,0 aus.

Ab Windows 10, Version 1607 und Windows Server 2016, wurde SSL 2,0 entfernt und wird nicht mehr unterstützt.

Änderungen an der Windows TLS-Einhaltung der TLS 1,2-Anforderungen für Verbindungen mit nicht kompatiblen TLS-Clients

In TLS 1,2 verwendet der Client die [Erweiterung "signature_algorithms"](#), um dem Server mitzuteilen, welche Signatur-/Hashalgorithmus-Paare in digitalen Signaturen (d. h. Server Zertifikate und Server Schlüsselaustausch) verwendet werden können. Die TLS 1,2-RFC erfordert auch, dass die Serverzertifikat-Nachricht die Erweiterung "signature_algorithms" berücksichtigt:

"Wenn der Client eine Erweiterung vom Typ "signature_algorithms" bereitgestellt hat, müssen alle vom Server bereitgestellten Zertifikate von einem Hash-/Signaturalgorithmuspaar signiert werden, das in dieser Erweiterung angezeigt wird.

In der Praxis entsprechen einige TLS-Clients von Drittanbietern nicht der TLS 1,2-RFC und können nicht alle Signatur- und Hash Algorithmus-Paare einschließen, die Sie in der Erweiterung "signature_algorithms" akzeptieren möchten, oder die Erweiterung weglassen (letztere gibt dem Server an, dass der Client nur SHA1 mit RSA, DSA oder ECDSA unterstützt).

Ein TLS-Server verfügt häufig nur über ein Zertifikat, das pro Endpunkt konfiguriert ist. Dies bedeutet, dass der Server nicht immer ein Zertifikat bereitstellen kann, das die Anforderungen des Clients erfüllt.

Vor Windows 10 und Windows Server 2016 hat der Windows TLS-Stapel streng den TLS 1,2 RFC-Anforderungen gerecht, was zu Verbindungsfehlern mit nicht kompatiblen RFC-Clients und Interoperabilitätsproblemen führt. In Windows 10 und Windows Server 2016 werden die Einschränkungen gelockert, und der Server kann ein Zertifikat senden, das nicht mit TLS 1,2 RFC übereinstimmt, wenn dies die einzige Option des Servers ist. Der Client kann dann den Handshake-Vorgang fortsetzen oder beenden.

Beim Validieren von Server- und Client-Zertifikaten erfüllt der Windows TLS-Stapel streng die TLS 1,2-RFC und lässt nur die ausgehandelte Signatur und die Hash-Algorithmen in den Server- und Client-Zertifikaten zu.

Verwalten von Transport Layer Security (TLS)

07.05.2020 • 9 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows 10

Konfigurieren der Reihenfolge der TLS-Verschlüsselungs Sammlungen

Unterschiedliche Windows-Versionen unterstützen verschiedene TLS-Verschlüsselungs Sammlungen und Prioritäts Reihenfolge. Weitere Informationen finden Sie unter Verschlüsselungs Sammlungen [in TLS/SSL \(Schannel SSP\)](#) für die Standard Reihenfolge, die vom Microsoft Schannel-Anbieter in verschiedenen Windows-Versionen unterstützt wird.

NOTE

Sie können auch die Liste der Verschlüsselungs Sammlungen mithilfe von CNG-Funktionen ändern. Weitere Informationen finden Sie unter [Priorisieren von Schannel Chiffre Suites](#).

Änderungen an der Reihenfolge der TLS-Verschlüsselungs Sammlungen werden beim nächsten Start wirksam. Bis zum Neustart oder zum Herunterfahren wird die vorhandene Bestellung wirksam.

WARNING

Das Aktualisieren der Registrierungs Einstellungen für die Standard Reihenfolge der Priorität wird nicht unterstützt und kann mit Wartungsupdates zurückgesetzt werden.

Konfigurieren der Reihenfolge der TLS-Verschlüsselungs Sammlung mithilfe von Gruppenrichtlinie

Sie können die Reihenfolge Gruppenrichtlinie Einstellungen der SSL-Verschlüsselungs Sammlung verwenden, um die Standard Reihenfolge der TLS-Verschlüsselungs Sammlung zu konfigurieren.

1. Wechseln Sie in der Gruppenrichtlinien-Verwaltungskontrolle zu **Computer Konfiguration > Administrative Vorlagen > Netzwerk > SSL-Konfigurationseinstellungen**.
2. Doppelklicken Sie auf die **Reihenfolge der SSL-Verschlüsselungs Sammlungen**, und klicken Sie dann auf die Option **aktiviert**.
3. Klicken Sie mit der rechten Maustaste auf das Feld **SSL -Verschlüsselungs Sammlungen**, und wählen Sie im Pop-upmenü die Option **Alle auswählen** aus.

4. Klicken Sie mit der rechten Maustaste auf den ausgewählten Text, und wählen Sie im Popup Menü **Kopieren** aus.
5. Fügen Sie den Text in einen Texteditor ein, z. b. "Notepad. exe", und aktualisieren Sie ihn mit der neuen Liste der Verschlüsselungs Sammlungen.

NOTE

Die Reihen folgen Liste der TLS-Verschlüsselungs Sammlung muss ein strenges Komma getrenntes Format aufweisen. Jede Chiffre Zeichenfolge endet mit einem Komma (,) auf der rechten Seite.

Außerdem ist die Liste der Verschlüsselungs Sammlungen auf 1.023 Zeichen beschränkt.

6. Ersetzen Sie die Liste in den SSL -Verschlüsselungs Sammlungen durch die aktualisierte geordnete Liste.
7. Klicken Sie auf **OK** oder **Übernehmen**.

Konfigurieren der Reihenfolge der TLS-Verschlüsselungs Sammlungen mithilfe von MDM

Der Windows 10 Policy CSP unterstützt die Konfiguration der TLS-Verschlüsselungs Sammlungen. Weitere Informationen finden Sie unter [Cryptography/tlsciphersuites](#) .

Konfigurieren der Reihenfolge der TLS-Verschlüsselungs Sammlungen mithilfe von TLS-PowerShell-Cmdlets

Das TLS-PowerShell-Modul unterstützt das Erhalten der geordneten Liste von TLS-Verschlüsselungs Sammlungen, das Deaktivieren einer Verschlüsselungs Sammlung und das Aktivieren einer Verschlüsselungs Sammlung. Weitere Informationen finden Sie unter [TLS-Modul](#) .

Konfigurieren der TLS ECC-Kurven Reihenfolge

Ab Windows 10 & Windows Server 2016 kann die ECC-Kurven Reihenfolge unabhängig von der Reihenfolge der Verschlüsselungs Sammlungen konfiguriert werden. Wenn die Reihen folgen Liste der TLS-Verschlüsselungs Sammlungen elliptische Kurven Suffixe aufweist, werden Sie bei Aktivierung durch die neue Priorität der elliptischen Kurven Priorität überschrieben. Dies ermöglicht es Organisationen, mithilfe eines Gruppenrichtlinie Objekts verschiedene Versionen von Windows mit der gleichen Chiffre Reihenfolge zu konfigurieren.

NOTE

Vor Windows 10 wurden Chiffre Sammlungs Zeichenfolgen mit der elliptischen Kurve angehängt, um die Kurven Priorität zu bestimmen.

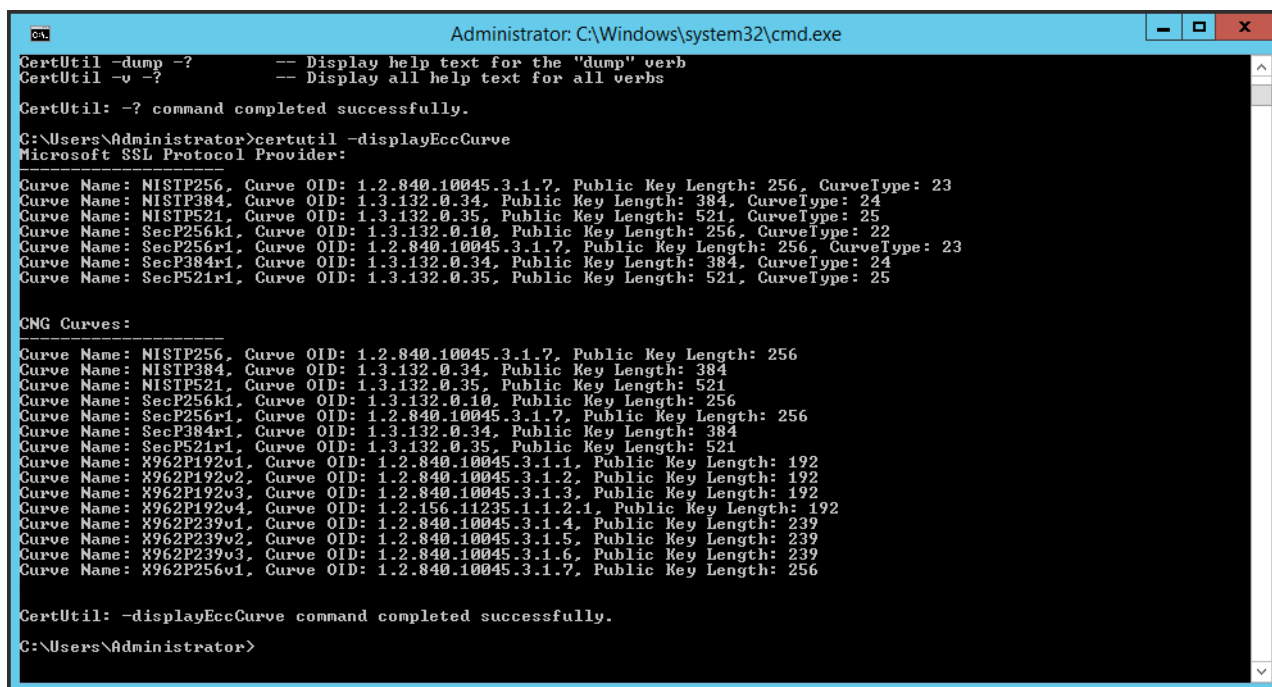
Verwalten von Windows ECC-Kurven mithilfe von certutil

Ab Windows 10 und Windows Server 2016 bietet Windows eine elliptische Kurven Parameter Verwaltung über das Befehlszeilen-Hilfsprogramm certutil.exe. Parameter der elliptischen Kurve werden in der Datei "bcryptprimitives.dll" gespeichert. Mithilfe von certutil.exe können Administratoren Kurven Parameter zu bzw. aus Windows hinzufügen bzw. daraus entfernen. Certutil.exe speichert die Kurven Parameter sicher in der Registrierung. Windows kann die Kurven Parameter mit dem Namen verwenden, der mit der Kurve verknüpft ist.

Anzeigen von registrierten Kurven

Verwenden Sie den folgenden certutil.exe-Befehl, um eine Liste der Kurven anzuzeigen, die für den aktuellen Computer registriert sind.

```
certutil.exe -displayEccCurve
```



```
Administrator: C:\Windows\system32\cmd.exe
CertUtil -dump -?      -- Display help text for the "dump" verb
CertUtil -v -?        -- Display all help text for all verbs

CertUtil: -? command completed successfully.

C:\Users\Administrator>certutil -displayEccCurve
Microsoft SSL Protocol Provider:
Curve Name: NISTP256, Curve OID: 1.2.840.10045.3.1.7, Public Key Length: 256, CurveType: 23
Curve Name: NISTP384, Curve OID: 1.3.132.0.34, Public Key Length: 384, CurveType: 24
Curve Name: NISTP521, Curve OID: 1.3.132.0.35, Public Key Length: 521, CurveType: 25
Curve Name: SecP256k1, Curve OID: 1.3.132.0.10, Public Key Length: 256, CurveType: 22
Curve Name: SecP256r1, Curve OID: 1.2.840.10045.3.1.7, Public Key Length: 256, CurveType: 23
Curve Name: SecP384r1, Curve OID: 1.3.132.0.34, Public Key Length: 384, CurveType: 24
Curve Name: SecP521r1, Curve OID: 1.3.132.0.35, Public Key Length: 521, CurveType: 25

CNG Curves:
Curve Name: NISTP256, Curve OID: 1.2.840.10045.3.1.7, Public Key Length: 256
Curve Name: NISTP384, Curve OID: 1.3.132.0.34, Public Key Length: 384
Curve Name: NISTP521, Curve OID: 1.3.132.0.35, Public Key Length: 521
Curve Name: SecP256k1, Curve OID: 1.3.132.0.10, Public Key Length: 256
Curve Name: SecP256r1, Curve OID: 1.2.840.10045.3.1.7, Public Key Length: 256
Curve Name: SecP384r1, Curve OID: 1.3.132.0.34, Public Key Length: 384
Curve Name: SecP521r1, Curve OID: 1.3.132.0.35, Public Key Length: 521
Curve Name: X962P192v1, Curve OID: 1.2.840.10045.3.1.1, Public Key Length: 192
Curve Name: X962P192v2, Curve OID: 1.2.840.10045.3.1.2, Public Key Length: 192
Curve Name: X962P192v3, Curve OID: 1.2.840.10045.3.1.3, Public Key Length: 192
Curve Name: X962P192v4, Curve OID: 1.2.156.1.1235.1.1.2.1, Public Key Length: 192
Curve Name: X962P239v1, Curve OID: 1.2.840.10045.3.1.4, Public Key Length: 239
Curve Name: X962P239v2, Curve OID: 1.2.840.10045.3.1.5, Public Key Length: 239
Curve Name: X962P239v3, Curve OID: 1.2.840.10045.3.1.6, Public Key Length: 239
Curve Name: X962P256v1, Curve OID: 1.2.840.10045.3.1.7, Public Key Length: 256

CertUtil: -displayEccCurve command completed successfully.
C:\Users\Administrator>
```

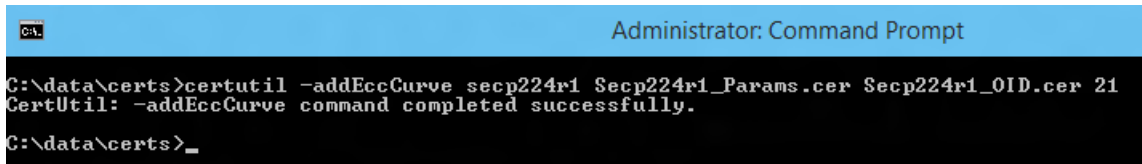
Abbildung 1: die Ausgabe von "Certutil.exe", um die Liste der registrierten Kurven anzuzeigen.

Hinzufügen einer neuen Kurve

Organisationen können Kurven Parameter erstellen und verwenden, die von anderen vertrauenswürdigen Entitäten erforscht werden. Administratoren, die diese neuen Kurven in Windows verwenden möchten, müssen die Kurve hinzufügen. Verwenden Sie den folgenden certutil.exe-Befehl, um dem aktuellen Computer eine Kurve hinzuzufügen:

```
Certutil -addEccCurve curveName curveParameters [curveOID] [curveType]
```

- Das **Cursor Name**-Argument stellt den Namen der Kurve dar, in der die Kurven Parameter hinzugefügt wurden.
- Das Argument "**curveParameters**" stellt den Dateinamen eines Zertifikats dar, das die Parameter der Kurven enthält, die Sie hinzufügen möchten.
- Das Argument "**curveoid**" stellt einen Dateinamen eines Zertifikats dar, das die OID der Kurven Parameter enthält, die Sie hinzufügen möchten (optional).
- Das **Cursor Type**-Argument stellt einen Dezimalwert der benannten Kurve aus dem [EC](#) (optional) dar.



```
C:\data\certs>certutil -addEccCurve secp224r1 Secp224r1_Params.cer Secp224r1_OID.cer 21
CertUtil: -addEccCurve command completed successfully.
C:\data\certs>_
```

Abbildung 2: Hinzufügen einer Kurve mithilfe von "Certutil.exe".

Entfernen einer zuvor hinzugefügten Kurve

Administratoren können eine zuvor hinzugefügte Kurve mit dem folgenden certutil.exe-Befehl entfernen:

```
Certutil.exe -deleteEccCurve curveName
```

Eine benannte Kurve kann nicht verwendet werden, nachdem ein Administrator die Kurve vom Computer entfernt hat.

Verwalten von Windows ECC-Kurven mithilfe von Gruppenrichtlinie

Organisationen können Kurven Parameter mithilfe von Gruppenrichtlinie und der Registrierungs Erweiterung Gruppenrichtlinie Einstellungen an Enterprise, in eine Domäne eingebundenen Computer verteilen. Der Prozess zum Verteilen einer Kurve ist:

1. Verwenden Sie unter Windows 10 und Windows Server 2016 "**certutil.exe**", um Windows eine neue registrierte benannte Kurve hinzuzufügen.
2. Öffnen Sie auf demselben Computer die Gruppenrichtlinien-Verwaltungskonsolle (GPMC), erstellen Sie ein neues Gruppenrichtlinie Objekt, und bearbeiten Sie es.
3. Navigieren Sie zu **Computer Konfiguration | Einstellungen | Windows-Einstellungen | Registrierung**. Klicken mit der rechten Maustaste auf **Registrierung**. Zeigen Sie auf **neu**, und wählen Sie **Sammel Element** aus. Benennen Sie das Sammel Element so um, dass es dem Namen der Kurve entspricht. Sie erstellen ein Registrierungs Sammel Element für jeden Registrierungsschlüssel unter `HKEY_LOCAL_MACHINE \currentcontrolset\control\cryptography\eccparameters`.
4. Konfigurieren Sie die neu erstellte Gruppenrichtlinie Einstellungs Registrierungs Sammlung, indem Sie ein neues **Registrierungs Element** für jeden Registrierungs Wert hinzufügen, der unter `HKEY_LOCAL_MACHINE \currentcontrolset\control\cryptography\eccparameters[Cursor Name]` aufgeführt ist.
5. Stellen Sie das Gruppenrichtlinie Objekt, das Gruppenrichtlinie Registrierungs Sammel Element enthält, für Windows 10- und Windows Server 2016-Computer bereit, die die neuen benannten Kurven erhalten sollen.

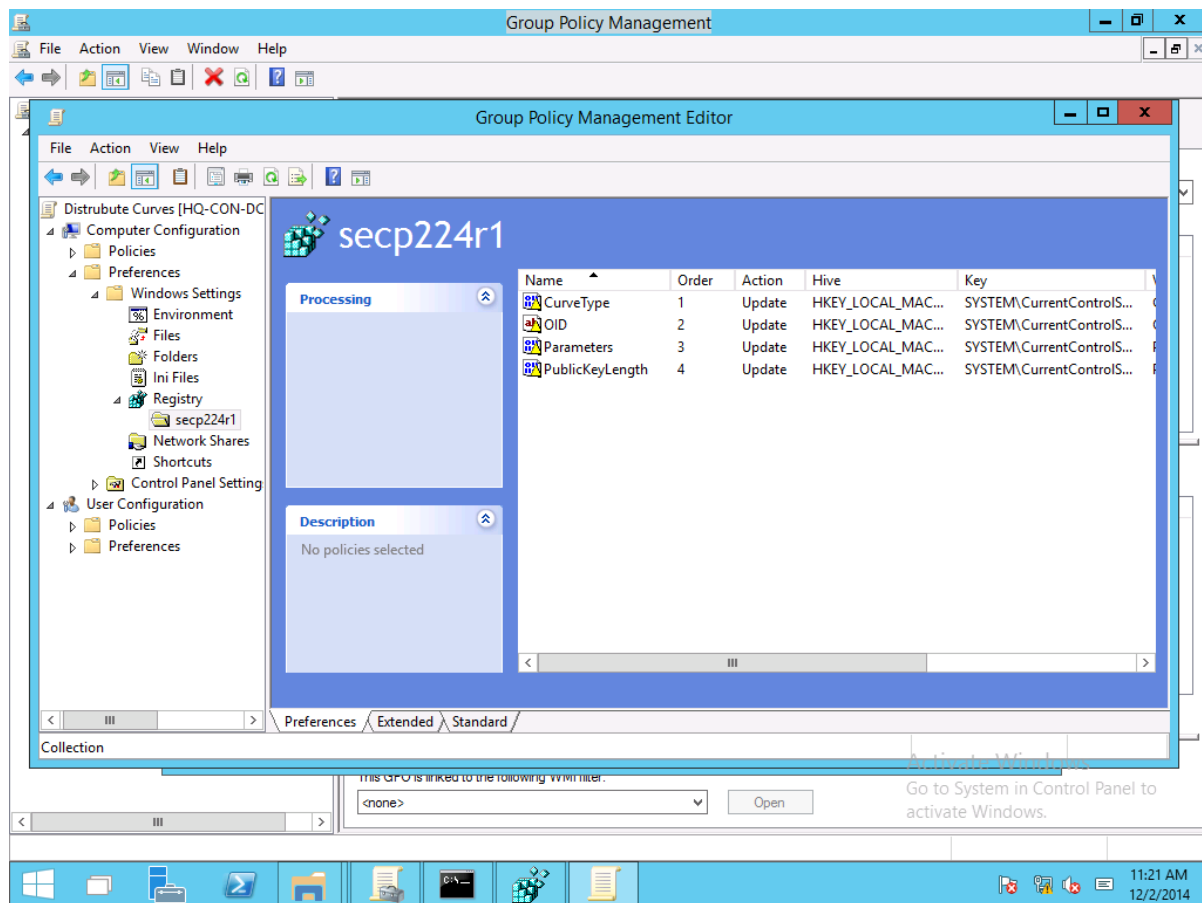


Abbildung 3 Verwenden von Gruppenrichtlinie Einstellungen zum Verteilen von Kurven

Verwalten der TLS ECC-Reihenfolge

Ab Windows 10 und Windows Server 2016 können die Gruppenrichtlinien Einstellungen für die ECC-Kurven Sortierung verwendet werden, um die standardmäßige TLS ECC-Kurven Reihenfolge zu konfigurieren. Mithilfe des generischen ECC und dieser Einstellung können Organisationen eigene vertrauenswürdige benannte Kurven (die für die Verwendung mit TLS genehmigt werden) dem Betriebssystem hinzufügen und diese benannten Kurven dann der Kurven Prioritäts Gruppenrichtlinie Einstellung hinzufügen, um sicherzustellen, dass Sie in zukünftigen TLS-Handshakes verwendet werden. Neue Kurven Prioritäts Listen werden beim nächsten Neustart nach dem Empfang der Richtlinien Einstellungen aktiv.

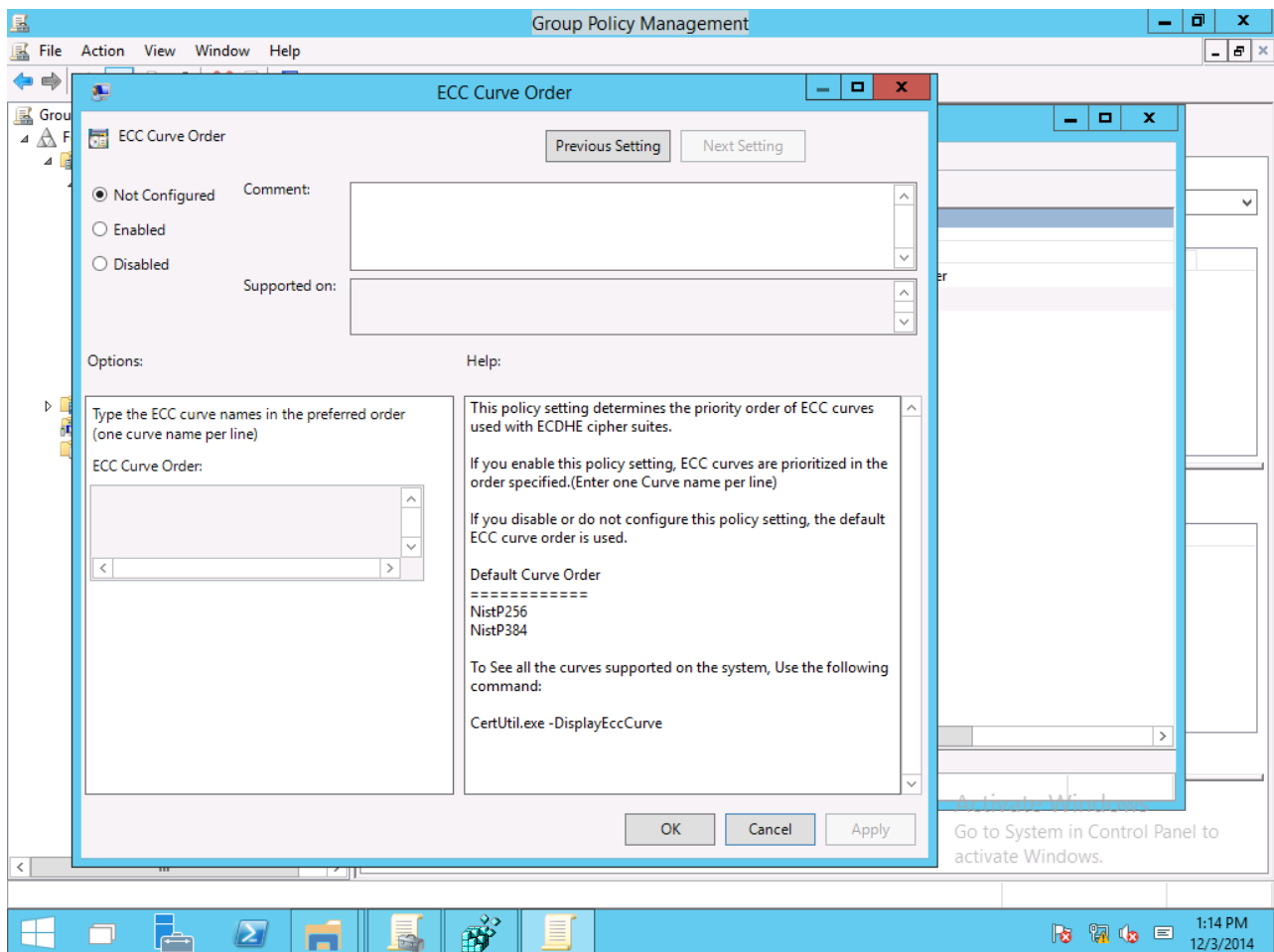


Abbildung 4 Verwalten der TLS-Kurven Priorität mithilfe Gruppenrichtlinie

Registrierungs Einstellungen für Transport Layer Security (TLS)

09.04.2020 • 34 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2019, Windows Server 2016, Windows 10

Dieses Referenz Thema für IT-Experten enthält unterstützte Registrierungs Einstellungs Informationen für die Windows-Implementierung des Transport Layer Security (TLS)-Protokolls und das Secure Sockets Layer (SSL)-Protokoll über den SChannel Security Support Provider (SSP). Die in diesem Thema behandelten Registrierungs Unterschlüssel und Einträge helfen Ihnen bei der Verwaltung und Problembehandlung des Schannel-SSP, insbesondere der TLS-und SSL-Protokolle.

Caution

Diese Informationen dienen als Referenz, die Sie nutzen, wenn Sie eine Problembehandlung durchführen oder prüfen, ob die erforderlichen Einstellungen vorhanden sind. Es wird empfohlen, die Registrierung nur dann direkt zu bearbeiten, wenn es keine andere Alternative gibt. Änderungen an der Registrierung werden weder vom Registrierungs-Editor noch vom Windows-Betriebssystem überprüft, bevor sie angewendet werden. Daher können falsche Werte gespeichert werden, was zu nicht behebbaren Fehlern im System führen kann. Anstatt die Registrierung direkt zu bearbeiten, verwenden Sie nach Möglichkeit Gruppenrichtlinien oder andere Windows-Tools wie die Microsoft Management Console (MMC) zum Ausführen von Aufgaben. Wenn Sie die Registrierung bearbeiten müssen, gehen Sie äußerst umsichtig vor.

CertificateMappingMethods

Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Der Standardwert ist, dass alle vier unten aufgeführten Methoden für die Clientzertifikatzuordnung unterstützt werden.

Wenn eine Serveranwendung die Clientauthentifizierung anfordert, versucht Schannel automatisch das Zertifikat, das vom Clientcomputer bereitgestellt wird, einem Benutzerkonto zuzuordnen. Sie können Benutzer authentifizieren, die sich mit einem Clientzertifikat anmelden, indem Sie Zuordnungen erstellen, die die Zertifikatsinformationen einem Windows-Benutzerkonto zuordnen. Nachdem Sie eine Zertifikatzuordnung erstellt und aktiviert haben, ordnet Ihre Serveranwendung immer dann, wenn ein Client ein Clientzertifikat vorlegt, diesen Benutzer dem entsprechenden Windows-Benutzerkonto zu.

In den meisten Fällen wird ein Zertifikat einem Benutzerkonto auf eine von zwei Arten zugeordnet:

- Ein einzelnes Zertifikat wird einem einzelnen Benutzerkonto zugeordnet (1:1-Zuordnung).
- Mehrere Zertifikate werden einem Benutzerkonto zugeordnet (n:1-Zuordnung).

Der Schannel-Anbieter verwendet standardmäßig die folgenden vier Methoden für die Clientzertifikatzuordnung, die nach Priorität aufgeführt sind:

1. Kerberos-S4U-Clientzertifikatzuordnung (Service-for-User)
2. Zuordnung von Benutzerprinzipalnamen
3. 1:1-Zuordnung (auch bekannt als Antragsteller/Aussteller- Zuordnung)
4. n:1-Zuordnung

Zutreffende Versionen: entsprechend der Angabe in der Liste **betrifft** am Anfang dieses Themas.

Registrierungs Pfad: HKLM system\currentcontrolset\control\securityproviders\schannel

Ciphers

TLS/SSL-Chiffren sollten gesteuert werden, indem die Reihenfolge der Verschlüsselungs Sammlungen konfiguriert wird. Weitere Informationen finden Sie unter [Konfigurieren der Reihenfolge der TLS-Verschlüsselungs Sammlungen](#).

Weitere Informationen über die Reihenfolge der Standard Verschlüsselungs Sammlungen, die vom Schannel SSP verwendet werden, finden Sie unter Verschlüsselungs Sammlungen [in TLS/SSL \(Schannel SSP\)](#).

CipherSuites

Das Konfigurieren von TLS/SSL-Verschlüsselungs Sammlungen sollte mithilfe von Gruppenrichtlinien, MDM oder PowerShell erfolgen. Weitere Informationen finden Sie unter [Konfigurieren der Reihenfolge der TLS - Verschlüsselungs Sammlungen](#).

Weitere Informationen über die Reihenfolge der Standard Verschlüsselungs Sammlungen, die vom Schannel SSP verwendet werden, finden Sie unter Verschlüsselungs Sammlungen [in TLS/SSL \(Schannel SSP\)](#).

ClientCacheTime

Dieser Eintrag steuert die Dauer in Millisekunden, die das Betriebssystem benötigt, um Einträge im clientseitigen Cache ablaufen zu lassen. Der Wert 0 deaktiviert das Zwischenspeichern sicherer Verbindungen. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden.

Wenn sich ein Client über den Schannel SSP erstmals mit einem Server verbindet, erfolgt ein vollständiger TLS/SSL-Handshake. Wenn dieser abgeschlossen ist, werden der geheime Hauptschlüssel, die Verschlüsselungssammlung und Zertifikate im Sitzungscache auf dem jeweiligen Client und Server gespeichert.

Ab Windows Server 2008 und Windows Vista beträgt die standardmäßige Client Cache Zeit 10 Stunden.

Registrierungs Pfad: HKLM system\currentcontrolset\control\securityproviders\schannel

Standardmäßige Clientcachezeiten

Enableocspstaplingforsni

Das Online Certificate Status-Protokoll (OCSP) ermöglicht einem Webserver, z. b. Internetinformationsdienste (IIS), den aktuellen Sperr Status eines Serverzertifikats bereitzustellen, wenn das Serverzertifikat während des TLS-Handshake an einen Client gesendet wird. Diese Funktion reduziert die Auslastung der OCSP-Server, da der Webserver den aktuellen OCSP-Status des Serverzertifikats Zwischenspeichern und an mehrere Webclients senden kann. Ohne diese Funktion würde jeder WebClient versuchen, den aktuellen OCSP-Status des Serverzertifikats vom OCSP-Server abzurufen. Dies würde eine hohe Auslastung auf diesem OCSP-Server generieren.

Zusätzlich zu IIS können auch Webdienste über http.sys von dieser Einstellung profitieren, einschließlich Active Directory-Verbunddienste (AD FS) (AD FS) und webanwendungsproxy (WAP).

Standardmäßig ist die OCSP-Unterstützung für IIS-Websites aktiviert, die über eine einfache sichere (SSL/TLS)-Bindung verfügen. Diese Unterstützung ist jedoch nicht standardmäßig aktiviert, wenn die IIS-Website einen oder beide der folgenden Typen von sicheren (SSL/TLS)-Bindungen verwendet:

- Servernamensanzeige anfordern
- Zentralisierten Zertifikatspeicher verwenden

In diesem Fall enthält die Server-Hello-Antwort während des TLS-Handshakes standardmäßig keinen OCSP-Status. Dieses Verhalten verbessert die Leistung: bei der Windows OCSP Heften-Implementierung werden hunderte von Server Zertifikaten skaliert. Da mit SNI und CCS IIS auf Tausende von Websites skaliert werden kann, die potenziell Tausende von Server Zertifikaten enthalten, kann das Festlegen dieses Verhaltensstandard mäßig zu

Leistungsproblemen führen.

Anwendbare Versionen: alle Versionen ab Windows Server 2012 und Windows 8.

Registrierungs Pfad: [HKEY_LOCAL_MACHINE \system\currentcontrolset\control\securityproviders\schannel]

Fügen Sie den folgenden Schlüssel hinzu:

"Enableocspstaplingforsni" = DWORD: 00000001

Legen Sie zum Deaktivieren von den DWORD-Wert auf 0 fest:

"Enableocspstaplingforsni" = DWORD: 00000000

NOTE

Die Aktivierung dieses Registrierungsschlüssels hat eine potenzielle Auswirkung auf die Leistung.

FIPSAgorithmPolicy

Dieser Eintrag steuert die FIPS-Einhaltung (Federal Information Processing Standard). Der Standard ist 0.

Anwendbare Versionen: alle Versionen ab Windows Server 2012 und Windows 8.

Registrierungs Pfad: HKLM SYSTEM\CurrentControlSet\Control\Lsa

Windows Server FIPS-Verschlüsselungs Sammlungen: Weitere Informationen finden Sie [unter Unterstützte Verschlüsselungs Sammlungen und Protokolle im Schannel-SSP](#).

Hashes

TLS/SSL-Hash Algorithmen sollten gesteuert werden, indem die Reihenfolge der Verschlüsselungs Sammlung konfiguriert wird. Weitere Informationen finden Sie unter [Konfigurieren der Reihenfolge der TLS -Verschlüsselungs Sammlungen](#).

IssuerCacheSize

Dieser Eintrag steuert die Größe des Ausstellercaches und wird mit der Ausstellerzuordnung verwendet. Der Schannel SSP versucht, alle Aussteller in der Zertifikat Kette des Clients zuzuordnen – nicht nur den direkten Aussteller des Client Zertifikats. Wenn die Aussteller keinem Konto zugeordnet werden, was der Normalfall ist, kann der Server versuchen, denselben Ausstellernamen wiederholt (unzählige Male pro Sekunde) zuzuordnen.

Um dies zu verhindern, hat der Server einen negativen Cache. Wenn also ein Ausstellernamen keinem Konto zugeordnet ist, wird er dem Cache hinzugefügt, woraufhin Schannel SSP nicht versucht, den Ausstellernamen erneut zuzuordnen, bis der Cacheeintrag abläuft. Dieser Registrierungseintrag gibt die Cachegröße an. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Der Standardwert ist 100.

Anwendbare Versionen: alle Versionen ab Windows Server 2008 und Windows Vista.

Registrierungs Pfad: HKLM system\currentcontrolset\control\securityproviders\schannel

IssuerCacheTime

Dieser Eintrag steuert das Zeitlimit für den Cache in Millisekunden. Der Schannel SSP versucht, alle Aussteller in der Zertifikat Kette des Clients zuzuordnen – nicht nur den direkten Aussteller des Client Zertifikats. Wenn die Aussteller keinem Konto zugeordnet werden, was der Normalfall ist, kann der Server versuchen, denselben Ausstellernamen wiederholt (unzählige Male pro Sekunde) zuzuordnen.

Um dies zu verhindern, hat der Server einen negativen Cache. Wenn also ein Ausstellernamen keinem Konto zugeordnet ist, wird er dem Cache hinzugefügt, woraufhin Schannel SSP nicht versucht, den Ausstellernamen erneut zuzuordnen, bis der Cacheeintrag abläuft. Dieser Cache wird aus Leistungsgründen eingerichtet, damit das System nicht laufend versucht, dieselben Aussteller zuzuordnen. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Der Standardwert beträgt 10 Minuten.

Anwendbare Versionen: alle Versionen ab Windows Server 2008 und Windows Vista.

Registrierungs Pfad: HKLM\system\currentcontrolset\control\securityproviders\schannel

Keyexchangealgorithmus-Client-RSA-Schlüsselgrößen

Dieser Eintrag steuert die Größe des RSA-Schlüssels für den Client.

Die Verwendung von Schlüsselaustausch Algorithmen sollte gesteuert werden, indem die Reihenfolge der Verschlüsselungs Sammlung konfiguriert wird.

In Windows 10, Version 1507 und Windows Server 2016 hinzugefügt.

Registrierungs Pfad:

hklm\system\currentcontrolset\control\securityproviders\schannel\keyexchangealgorithms\pkcs

Um einen minimal unterstützten Bereich der RSA-Schlüssel Bit Länge für den TLS-Client anzugeben, erstellen Sie einen **clientminkeybitlength** -Eintrag. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in die gewünschte Bitlänge. Wenn keine Konfiguration erfolgt, sind 1024 Bits das minimale.

Um einen maximalen unterstützten Bereich der RSA-Schlüssel Bit Länge für den TLS-Client anzugeben, erstellen Sie einen **clientmaxkeybitlength** -Eintrag. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in die gewünschte Bitlänge. Wenn diese nicht konfiguriert ist, wird ein Maximum nicht erzwungen.

Keyexchangealgorithmus-Diffie-Hellman-Schlüsselgrößen

Dieser Eintrag steuert die Diffie-Hellman-Schlüsselgrößen.

Die Verwendung von Schlüsselaustausch Algorithmen sollte gesteuert werden, indem die Reihenfolge der Verschlüsselungs Sammlung konfiguriert wird.

In Windows 10, Version 1507 und Windows Server 2016 hinzugefügt.

Registrierungs Pfad:

hklm\system\currentcontrolset\control\securityproviders\schannel\keyexchangealgorithms\diffie-Hellman

Um einen minimal unterstützten Bereich von Diffie-Helman Key Bit length für den TLS-Client anzugeben, erstellen Sie einen **clientminkeybitlength** -Eintrag. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in die gewünschte Bitlänge. Wenn keine Konfiguration erfolgt, sind 1024 Bits das minimale.

Wenn Sie einen maximal unterstützten Bereich von Diffie-Helman Key Bit length für den TLS-Client angeben möchten, erstellen Sie einen **clientmaxkeybitlength** -Eintrag. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in die gewünschte Bitlänge. Wenn diese nicht konfiguriert ist, wird ein Maximum nicht erzwungen.

Erstellen Sie einen **serverminkeybitlength** -Eintrag, um die Diffie-Helman-Schlüssel Bit Länge für den TLS-Server Standard anzugeben. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in die gewünschte Bitlänge. Wenn diese Einstellung nicht konfiguriert ist, werden 2048 Bits als Standard verwendet.

MaximumCacheSize

Dieser Eintrag steuert die maximale Anzahl von Elementen im Cache. Durch Festlegen von "MaximumCacheSize" auf 0 werden der serverseitige Sitzungscache deaktiviert und erneute Verbindungen verhindert. Das Erhöhen von "MaximumCacheSize" über die Standardwerte hinaus bewirkt, dass "Lsass.exe" zusätzlichen Arbeitsspeicher beansprucht. Jedes Session-Cache-Element benötigt in der Regel 2 bis 4 KB Arbeitsspeicher. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Der Standardwert ist 20.000 Elemente.

Anwendbare Versionen: alle Versionen ab Windows Server 2008 und Windows Vista.

Registrierungspfad: HKLM\system\currentcontrolset\control\securityproviders\schannel

Messaging – fragmentverarbeitung

Dieser Eintrag steuert die maximal zulässige Größe von fragmentierten TLS-Handshake-Nachrichten, die akzeptiert werden. Nachrichten, die größer als die zulässige Größe sind, werden nicht akzeptiert, und der TLS-Handshake schlägt fehl. Diese Einträge sind nicht standardmäßig in der Registrierung vorhanden.

Wenn Sie den Wert auf 0x0 festlegen, werden fragmentierte Nachrichten nicht verarbeitet und bewirken, dass der TLS-Handshake fehlschlägt. Dadurch werden TLS-Clients oder-Server auf dem aktuellen Computer nicht mit den TLS-RFCs kompatibel.

Die maximal zulässige Größe kann bis zu $2^{24}-1$ Byte betragen. Es ist keine gute Idee, einem Client oder Server das Lesen und Speichern großer Mengen nicht überprüfter Daten aus dem Netzwerk zu ermöglichen, und es wird zusätzlicher Arbeitsspeicher für jeden Sicherheitskontext beansprucht.

Hinzugefügt in Windows 7 und Windows Server 2008 R2. Ein Update, mit dem Internet Explorer in Windows XP, Windows Vista oder Windows Server 2008 zur Analyse fragmentierter TLS/SSL-Handshake Nachrichten verwendet werden kann.

Registrierungspfad: hklm\system\currentcontrolset\control\securityproviders\schannel\messaging

Erstellen Sie einen **messagelimitclient** -Eintrag, um eine maximal zulässige Größe von fragmentierten TLS-Handshake Nachrichten anzugeben, die vom TLS-Client akzeptiert werden. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in die gewünschte Bitlänge. Wenn keine Konfiguration erfolgt, ist der Standardwert 0x8000 bytes.

Erstellen Sie einen **messagelimitserver** -Eintrag, um eine maximal zulässige Größe von fragmentierten TLS-Handshake Nachrichten anzugeben, die vom TLS-Server akzeptiert werden, wenn keine Client Authentifizierung vorhanden ist. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in die gewünschte Bitlänge. Wenn diese Einstellung nicht konfiguriert ist, wird der Standardwert 0x4000 Bytes betragen.

Zum Angeben einer maximal zulässigen Größe von fragmentierten TLS-Handshake-Nachrichten, die der TLS-Server bei der Client Authentifizierung akzeptieren wird, erstellen Sie einen **messagelimitserverclientauth** -Eintrag. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in die gewünschte Bitlänge. Wenn keine Konfiguration erfolgt, ist der Standardwert 0x8000 bytes.

SendTrustedIssuerList

Dieser Eintrag steuert das Kennzeichen, das verwendet wird, wenn die Liste der vertrauenswürdigen Aussteller gesendet wird. Bei Servern, die für die Clientauthentifizierung Hunderten von Zertifizierungsstellen vertrauen, gibt es zu viele Aussteller, die der Server nicht alle an den Clientcomputer senden kann, wenn die Clientauthentifizierung angefordert wird. In diesem Fall kann dieser Registrierungsschlüssel festgelegt werden. Anstatt eine Teilliste zu senden, sendet der Schannel SSP keine Liste an den Client.

Wenn keine Liste vertrauenswürdiger Aussteller gesendet wird, kann dies Auswirkungen darauf haben, was der Client sendet, wenn von ihm ein Clientzertifikat angefordert wird. Wenn z. B. Internet Explorer eine Anforderung für

die Clientauthentifizierung empfängt, zeigt der Browser nur Clientzertifikate an, die mit einer der Zertifizierungsstellen verkettet sind, die vom Server gesendet wird. Wenn der Server keine Liste gesendet hat, zeigt Internet Explorer alle Clientzertifikate, die auf dem Client installiert sind.

Dieses Verhalten ist möglicherweise wünschenswert. Wenn z. B. PKI-Umgebungen übergreifende Zertifikate enthalten, haben die Client- und Server-Zertifikate nicht die gleiche Stamm-Zertifizierungsstelle. Aus diesem Grund kann Internet Explorer kein Zertifikat auswählen, das mit einem der Server-CAS verknüpft ist. Indem Sie konfigurieren, dass der Server keine Liste der vertrauenswürdigen Aussteller sendet, sendet Internet Explorer alle seine Zertifikate.

Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden.

Standardverhalten der Liste vertrauenswürdiger Aussteller senden

| WINDOWS-VERSION | ZEIT |
|---|-------|
| Windows Server 2012 und Windows 8 und höher | FALSE |
| Windows Server 2008 R2 und Windows 7 und früher | TRUE |

Anwendbare Versionen: alle Versionen ab Windows Server 2008 und Windows Vista.

Registrierungspfad: HKLM system\currentcontrolset\control\securityproviders\schannel

ServerCacheTime

Dieser Eintrag steuert die Dauer, die das Betriebssystem in Millisekunden benötigt, um Einträge im serverseitigen Cache ablaufen zu lassen. Durch Festlegen auf 0 werden der serverseitige Sitzungscache deaktiviert und erneute Verbindungen verhindert. Das Erhöhen von "ServerCacheTime" über die Standardwerte bewirkt, dass "Lsass.exe" zusätzlichen Arbeitsspeicher beansprucht. Jedes Sitzungs-Cache-Element benötigt in der Regel 2 bis 4 KB Arbeitsspeicher. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden.

Anwendbare Versionen: alle Versionen ab Windows Server 2008 und Windows Vista.

Registrierungspfad: HKLM system\currentcontrolset\control\securityproviders\schannel

Standard Server Cache-Zeit: 10 Stunden

SSL 2.0

Dieser Unterschlüssel steuert die Verwendung von SSL 2,0.

Ab Windows 10, Version 1607 und Windows Server 2016, wurde SSL 2,0 entfernt und wird nicht mehr unterstützt. Die Standardeinstellungen für SSL 2,0 finden Sie unter [Protokolle in TLS/SSL \(Schannel SSP\)](#).

Registrierungspfad: HKLM system\currentcontrolset\control\securityproviders\schannel\protokolle

Um das SSL 2,0-Protokoll zu aktivieren, erstellen Sie einen **aktivierten** Eintrag im Client- oder Server-Unterschlüssel, wie in der folgenden Tabelle beschrieben. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in 1.

SSL 2,0-Unterschlüssel Tabelle

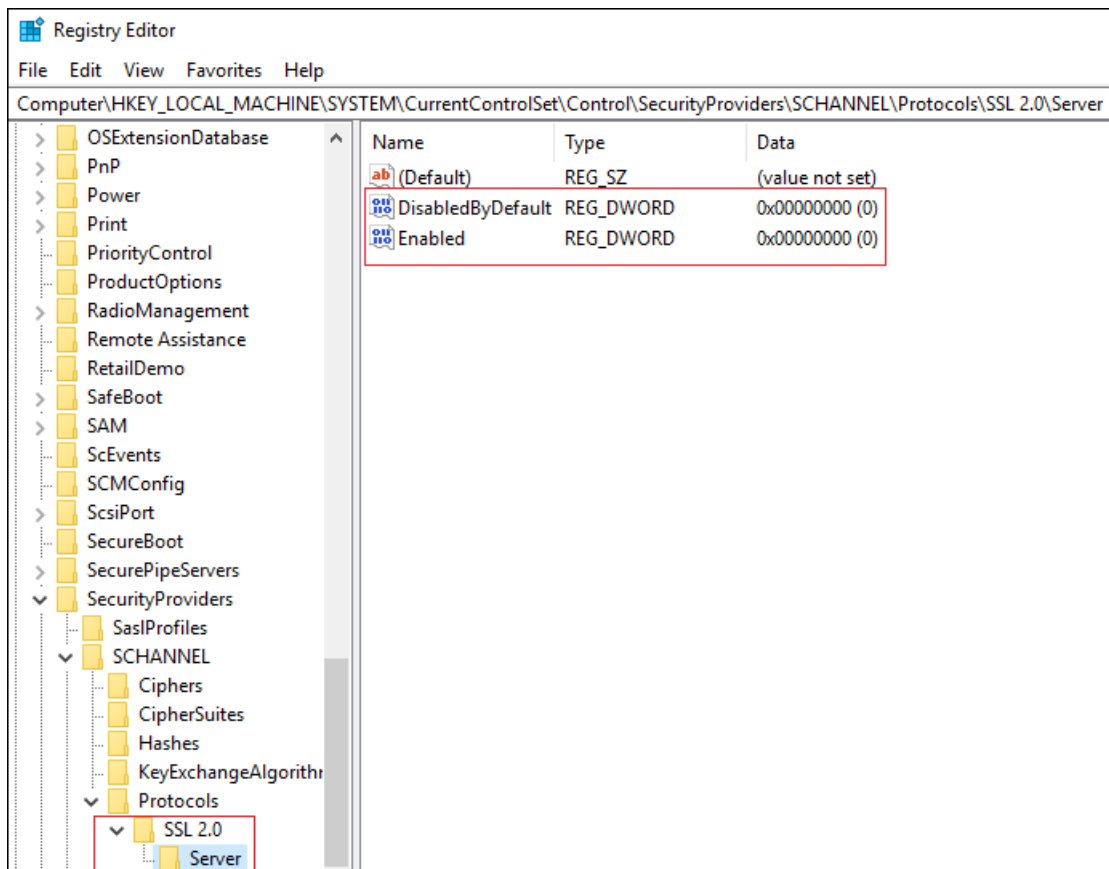
| UNTERSCHLÜSSEL | BESCHREIBUNG |
|----------------|--|
| Client | Steuert die Verwendung von SSL 2,0 auf dem SSL-Client. |

| UNTERSCHLÜSSEL | BESCHREIBUNG |
|----------------|--|
| Server | Steuert die Verwendung von SSL 2,0 auf dem SSL-Server. |

Um SSL 2,0 für Client oder Server zu deaktivieren, ändern Sie den DWORD-Wert in 0. Wenn eine SSPI-APP die Verwendung von SSL 2,0 anfordert, wird Sie verweigert.

Um SSL 2,0 standardmäßig zu deaktivieren, erstellen Sie einen **disabledbydefault** -Eintrag und ändern den DWORD-Wert in 1. Wenn eine SSPI-App für die Verwendung von SSL 2,0-Anforderungen aufgefordert wird, kann Sie ausgehandelt werden.

Das folgende Beispiel zeigt SSL 2,0, das in der Registrierung deaktiviert ist:



SSL 3.0

Dieser Unterschlüssel steuert die Verwendung von SSL 3,0.

Ab Windows 10, Version 1607 und Windows Server 2016, wurde SSL 3,0 standardmäßig deaktiviert. Die Standardeinstellungen für SSL 3,0 finden Sie unter [Protokolle in TLS/SSL \(Schannel SSP\)](#).

Registrierungs Pfad: HKLM system\currentcontrolset\control\securityproviders\schannel\protokolle

Um das SSL 3,0-Protokoll zu aktivieren, erstellen Sie einen **aktivierten** Eintrag im Client-oder Server-Unterschlüssel, wie in der folgenden Tabelle beschrieben.

Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in 1.

SSL 3,0-Unterschlüssel Tabelle

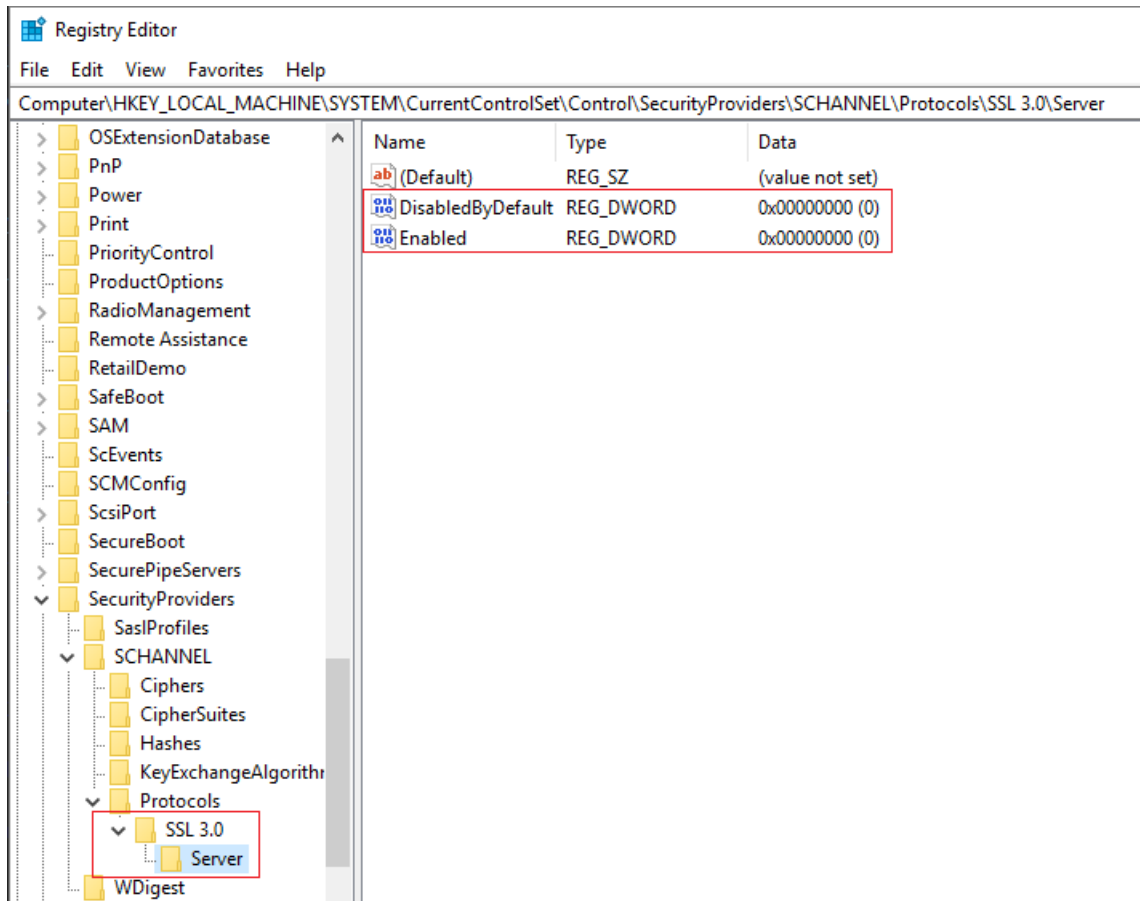
| UNTERSCHLÜSSEL | BESCHREIBUNG |
|----------------|--|
| Client | Steuert die Verwendung von SSL 3,0 auf dem SSL-Client. |

| UNTERSCHLÜSSEL | BESCHREIBUNG |
|----------------|--|
| Server | Steuert die Verwendung von SSL 3,0 auf dem SSL-Server. |

Um SSL 3,0 für Client oder Server zu deaktivieren, ändern Sie den DWORD-Wert in 0. Wenn eine SSPI-APP die Verwendung von SSL 3,0 anfordert, wird Sie verweigert.

Um SSL 3,0 standardmäßig zu deaktivieren, erstellen Sie einen **disabledbydefault** -Eintrag und ändern den DWORD-Wert in 1. Wenn eine SSPI-App explizit die Verwendung von SSL 3,0 anfordert, wird Sie möglicherweise ausgehandelt.

Das folgende Beispiel zeigt SSL 3,0, das in der Registrierung deaktiviert ist:



TLS 1.0

Dieser Unterschlüssel steuert die Verwendung von TLS 1,0.

Die Standardeinstellungen für TLS 1,0 finden Sie unter [Protokolle in TLS/SSL \(Schannel SSP\)](#).

Registrierungs Pfad: HKLM system\currentcontrolset\control\securityproviders\schannel\protokolle

Um das TLS 1,0-Protokoll zu aktivieren, erstellen Sie einen **aktivierten** Eintrag im Client-oder Server-Unterschlüssel, wie in der folgenden Tabelle beschrieben. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in 1.

TLS 1,0-Unterschlüssel Tabelle

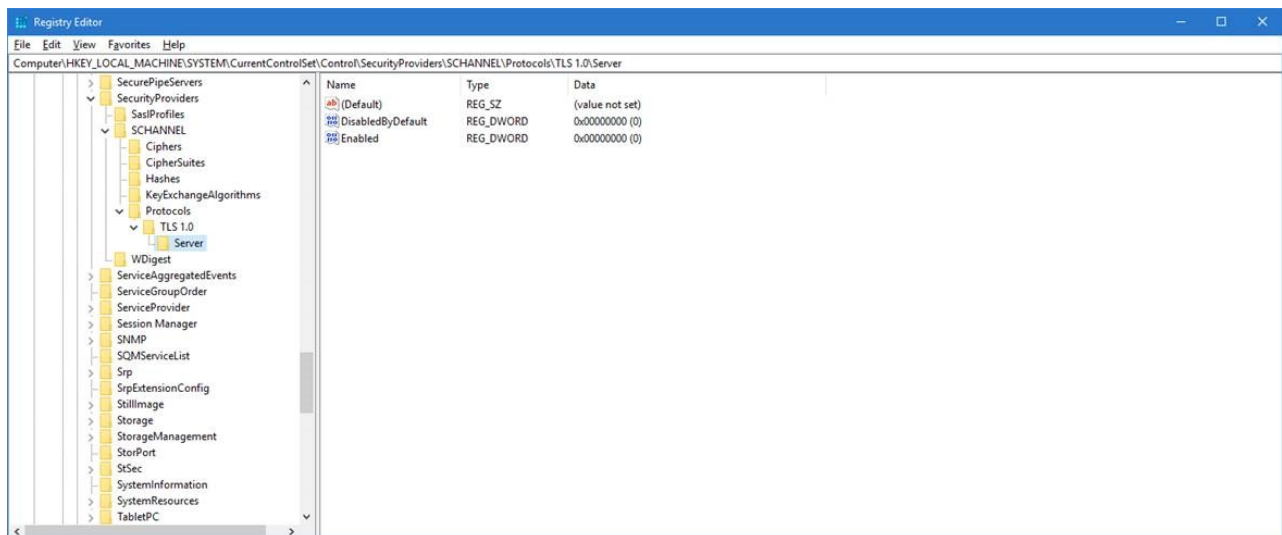
| UNTERSCHLÜSSEL | BESCHREIBUNG |
|----------------|--|
| Client | Steuert die Verwendung von TLS 1,0 auf dem TLS-Client. |

| UNTERSCHLÜSSEL | BESCHREIBUNG |
|----------------|--|
| Server | Steuert die Verwendung von TLS 1,0 auf dem TLS-Server. |

Um TLS 1,0 für Client oder Server zu deaktivieren, ändern Sie den DWORD-Wert in 0. Wenn eine SSPI-APP die Verwendung von TLS 1,0 anfordert, wird Sie verweigert.

Um TLS 1,0 standardmäßig zu deaktivieren, erstellen Sie einen **disabledbydefault** -Eintrag und ändern den DWORD-Wert in 1. Wenn eine SSPI-App explizit die Verwendung von TLS 1,0 anfordert, wird Sie möglicherweise ausgehandelt.

Im folgenden Beispiel wird das in der Registrierung deaktivierte TLS 1,0 angezeigt:



TLS 1.1

Dieser Unterschlüssel steuert die Verwendung von TLS 1,1.

Die Standardeinstellungen für TLS 1,1 finden Sie unter [Protokolle in TLS/SSL \(Schannel SSP\)](#).

Registrierungs Pfad: HKLM system\currentcontrolset\control\securityproviders\schannel\protokolle

Um das TLS 1,1-Protokoll zu aktivieren, erstellen Sie einen **aktivierten** Eintrag im Client-oder Server-Unterschlüssel, wie in der folgenden Tabelle beschrieben. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in 1.

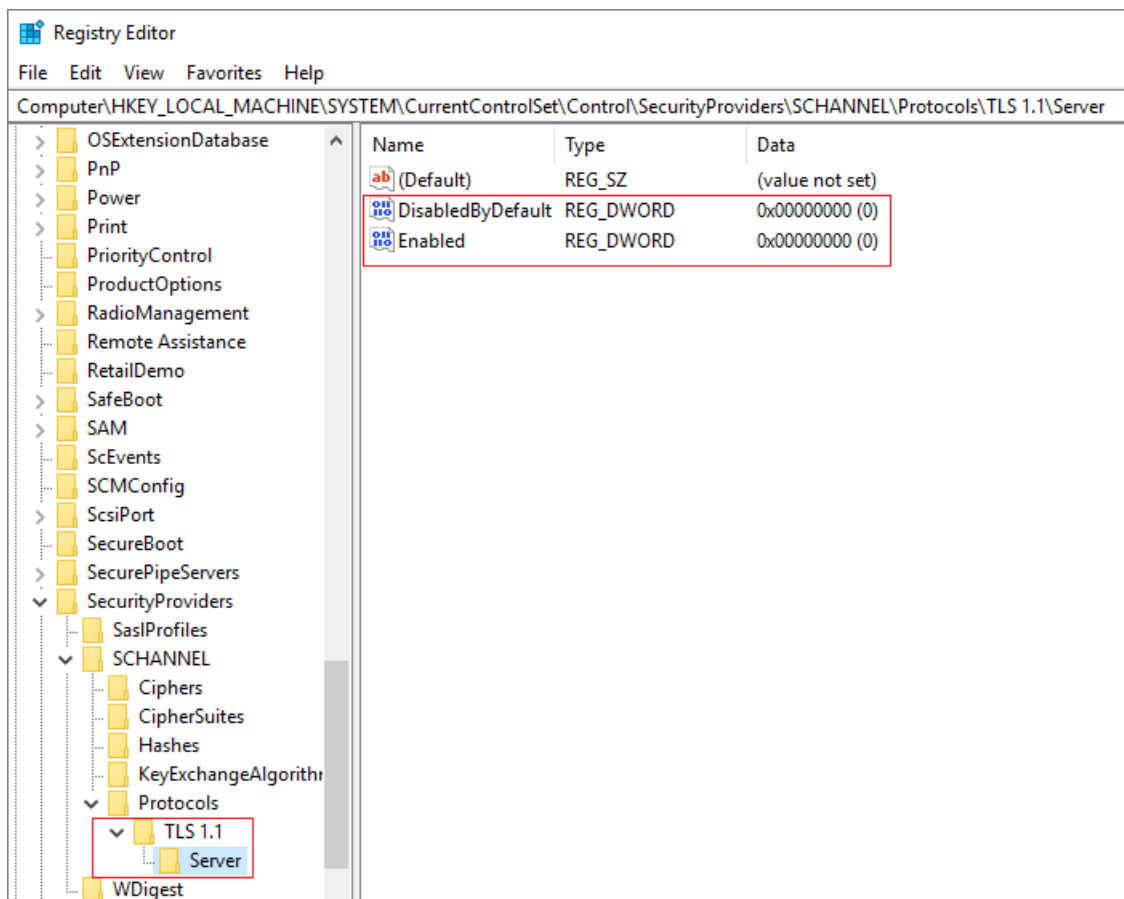
TLS 1,1-Unterschlüssel Tabelle

| UNTERSCHLÜSSEL | BESCHREIBUNG |
|----------------|--|
| Client | Steuert die Verwendung von TLS 1,1 auf dem TLS-Client. |
| Server | Steuert die Verwendung von TLS 1,1 auf dem TLS-Server. |

Um TLS 1,1 für Client oder Server zu deaktivieren, ändern Sie den DWORD-Wert in 0. Wenn eine SSPI-APP die Verwendung von TLS 1,1 anfordert, wird Sie verweigert.

Um TLS 1,1 standardmäßig zu deaktivieren, erstellen Sie einen **disabledbydefault** -Eintrag und ändern den DWORD-Wert in 1. Wenn eine SSPI-App explizit die Verwendung von TLS 1,1 anfordert, wird Sie möglicherweise ausgehandelt.

Im folgenden Beispiel wird das in der Registrierung deaktivierte TLS 1,1 angezeigt:



TLS 1.2

Dieser Unterschlüssel steuert die Verwendung von TLS 1,2.

Die Standardeinstellungen für TLS 1,2 finden Sie unter [Protokolle in TLS/SSL \(Schannel SSP\)](#).

Registrierungs Pfad: HKLM system\currentcontrolset\control\securityproviders\schannel\protokolle

Um das TLS 1,2-Protokoll zu aktivieren, erstellen Sie einen **aktivierten** Eintrag im Client-oder Server-Unterschlüssel, wie in der folgenden Tabelle beschrieben. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in 1.

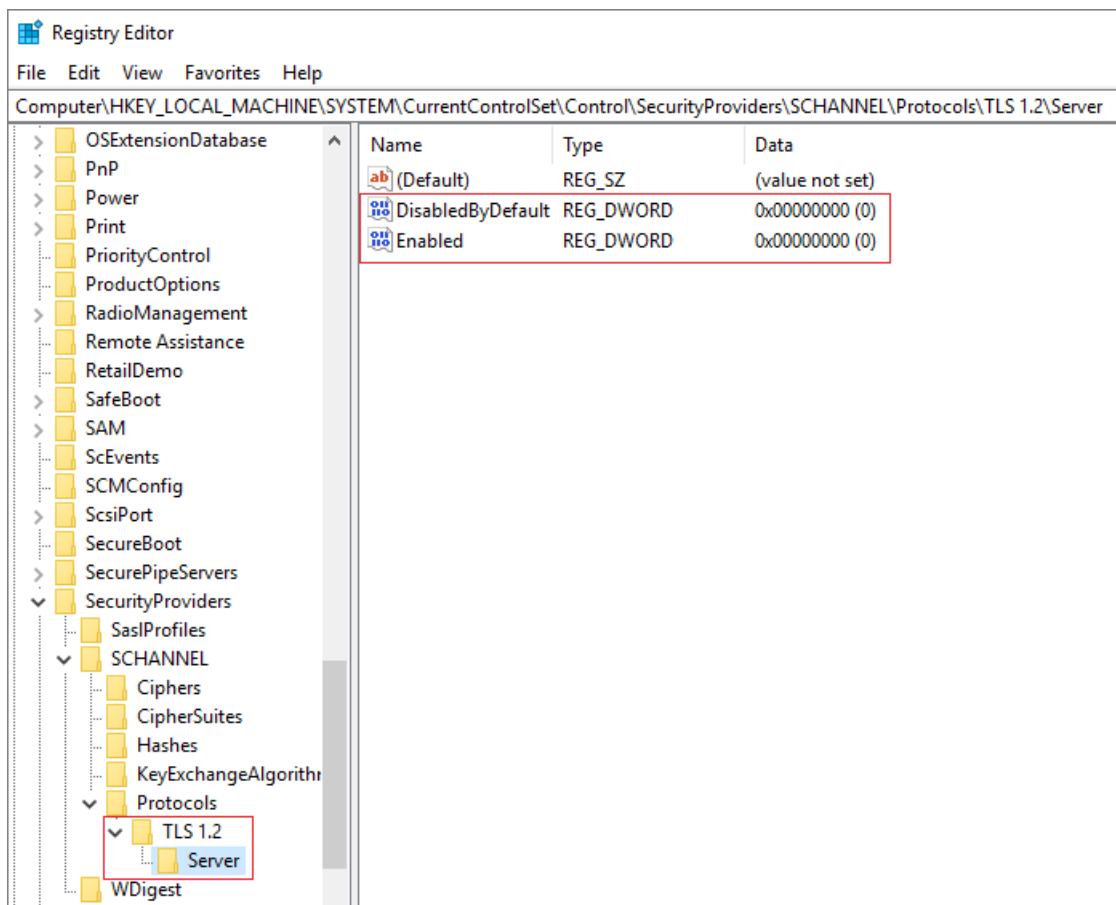
TLS 1,2-Unterschlüssel Tabelle

| UNTERSCHLÜSSEL | BESCHREIBUNG |
|----------------|--|
| Client | Steuert die Verwendung von TLS 1,2 auf dem TLS-Client. |
| Server | Steuert die Verwendung von TLS 1,2 auf dem TLS-Server. |

Um TLS 1,2 für Client oder Server zu deaktivieren, ändern Sie den DWORD-Wert in 0. Wenn eine SSPI-APP die Verwendung von TLS 1,2 anfordert, wird Sie verweigert.

Um TLS 1,2 standardmäßig zu deaktivieren, erstellen Sie einen **disabledbydefault** -Eintrag und ändern den DWORD-Wert in 1. Wenn eine SSPI-App explizit die Verwendung von TLS 1,2 anfordert, wird Sie möglicherweise ausgehandelt.

Im folgenden Beispiel wird das in der Registrierung deaktivierte TLS 1,2 angezeigt:



DTLS 1.0

Dieser Unterschlüssel steuert die Verwendung von DTLS 1,0.

Die Standardeinstellungen für DTLS 1,0 finden Sie unter [Protokolle in TLS/SSL \(Schannel SSP\)](#).

Registrierungs Pfad: HKLM system\currentcontrolset\control\securityproviders\schannel\protokolle

Um das DTLS 1,0-Protokoll zu aktivieren, erstellen Sie einen **aktivierten** Eintrag im Client-oder Server-Unterschlüssel, wie in der folgenden Tabelle beschrieben. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in 1.

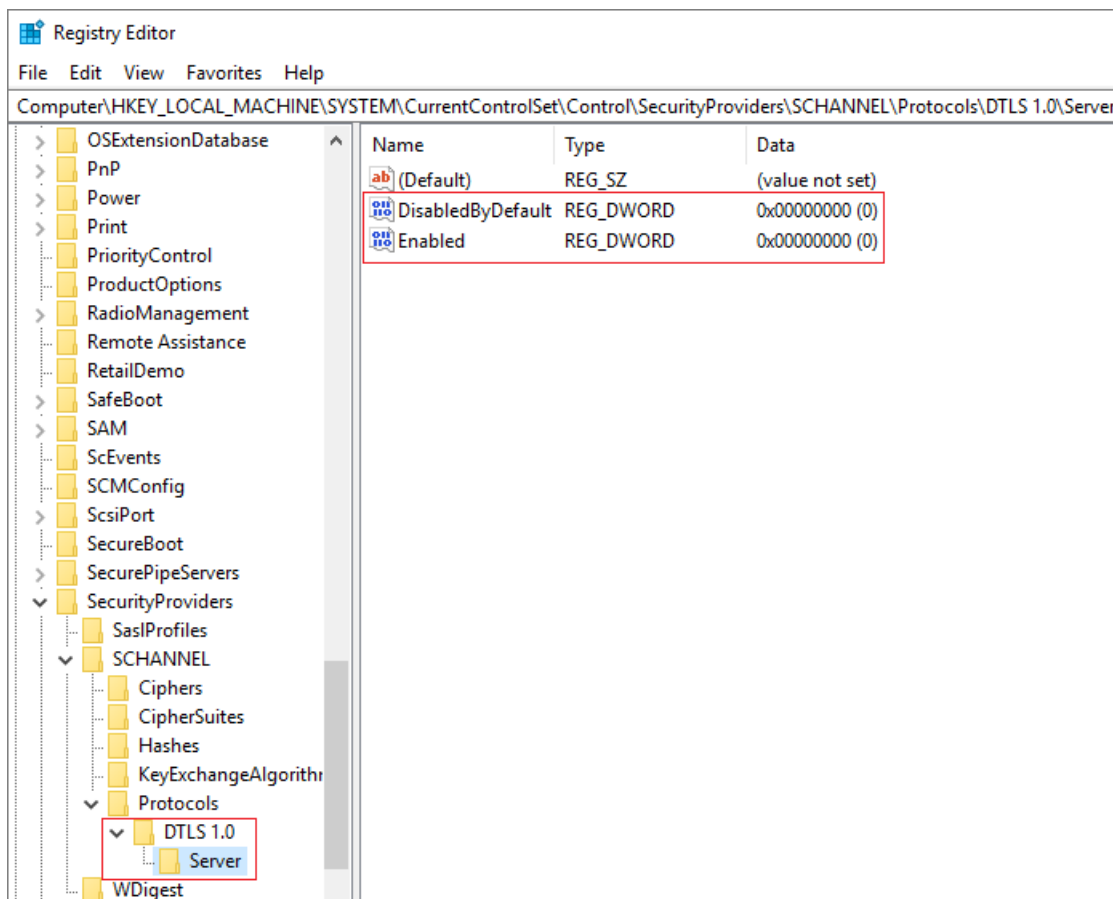
DTLS 1,0-Unterschlüssel Tabelle

| UNTERSCHLÜSSEL | BESCHREIBUNG |
|----------------|--|
| Client | Steuert die Verwendung von DTLS 1,0 auf dem DTLS-Client. |
| Server | Steuert die Verwendung von DTLS 1,0 auf dem DTLS-Server. |

Um DTLS 1,0 für Client oder Server zu deaktivieren, ändern Sie den DWORD-Wert in 0. Wenn eine SSPI-APP die Verwendung von DTLS 1,0 anfordert, wird Sie verweigert.

Um DTLS 1,0 standardmäßig zu deaktivieren, erstellen Sie einen **disabledbydefault** -Eintrag und ändern den DWORD-Wert in 1. Wenn eine SSPI-App explizit die Verwendung von DTLS 1,0 anfordert, wird Sie möglicherweise ausgehandelt.

Im folgenden Beispiel wird die in der Registrierung deaktivierte DTLS 1,0 angezeigt:



DTLS 1,2

Dieser Unterschlüssel steuert die Verwendung von DTLS 1,2.

Die Standardeinstellungen für DTLS 1,2 finden Sie unter [Protokolle in TLS/SSL \(Schannel SSP\)](#).

Registrierungs Pfad: HKLM system\currentcontrolset\control\securityproviders\schannel\protokolle

Um das DTLS 1,2-Protokoll zu aktivieren, erstellen Sie einen **aktivierten** Eintrag im Client-oder Server-Unterschlüssel, wie in der folgenden Tabelle beschrieben. Dieser Eintrag ist nicht standardmäßig in der Registrierung vorhanden. Nachdem Sie den Eintrag erstellt haben, ändern Sie den DWORD-Wert in 1.

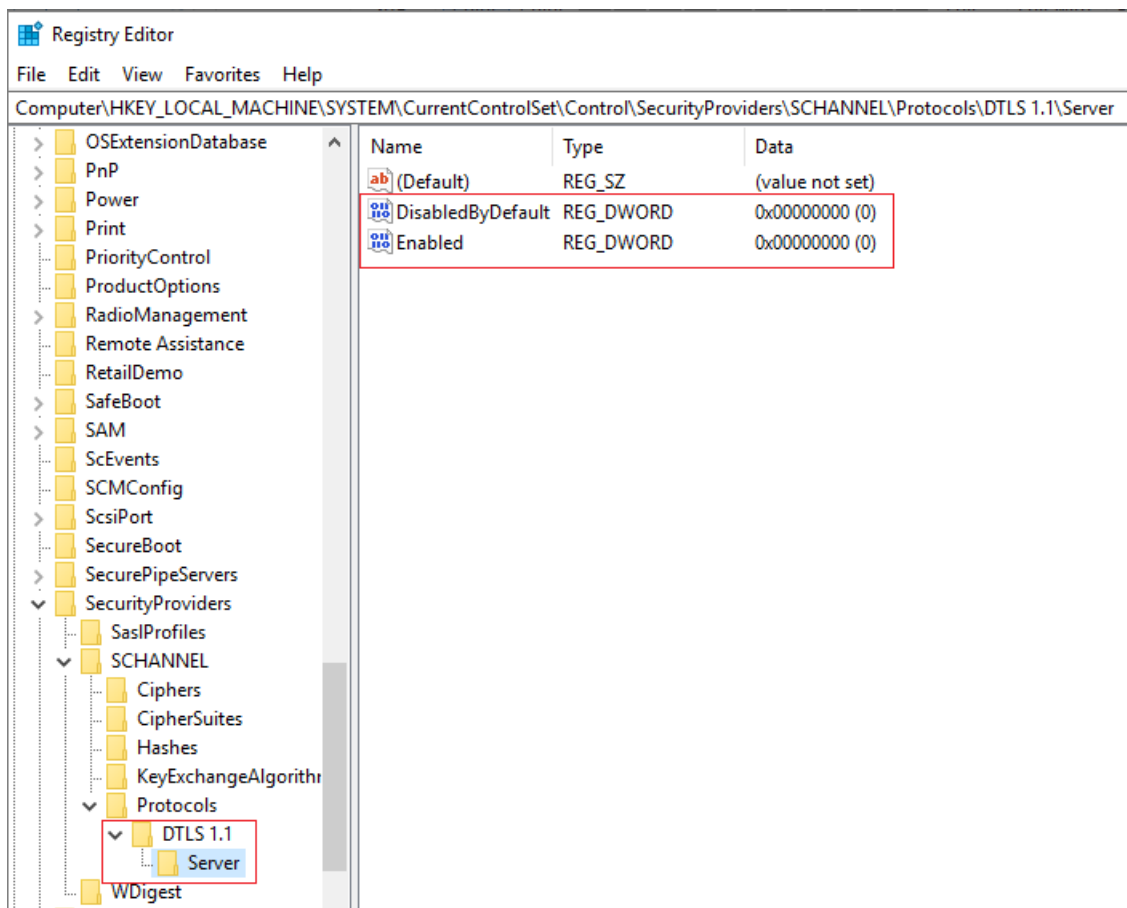
DTLS 1,2-Unterschlüssel Tabelle

| UNTERSCHLÜSSEL | BESCHREIBUNG |
|----------------|--|
| Client | Steuert die Verwendung von DTLS 1,2 auf dem DTLS-Client. |
| Server | Steuert die Verwendung von DTLS 1,2 auf dem DTLS-Server. |

Um DTLS 1,2 für Client oder Server zu deaktivieren, ändern Sie den DWORD-Wert in 0. Wenn eine SSPI-APP die Verwendung von DTLS 1,0 anfordert, wird Sie verweigert.

Um DTLS 1,2 standardmäßig zu deaktivieren, erstellen Sie einen **disabledbydefault** -Eintrag und ändern den DWORD-Wert in 1. Wenn eine SSPI-App explizit die Verwendung von DTLS 1,2 anfordert, wird Sie möglicherweise ausgehandelt.

Im folgenden Beispiel wird die in der Registrierung deaktivierte DTLS 1,1 angezeigt:



Schannel Security Support Provider: Technische Referenz

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows 10

Diese Referenz für IT-Experten enthält Informationen über das Transport Layer Security (TLS)-Protokoll, das Secure Sockets Layer (SSL)-Protokoll und das DTLS-Protokoll (Datagram Transport Layer Security), das vom Schannel Security Support Provider (SSP) implementiert wird.

Diese Protokolle bieten eine Möglichkeit zum Sichern von Daten, die zwischen Anwendungen in einem nicht vertrauenswürdigen Netzwerk gesendet werden, mithilfe von Zertifikat basierter Authentifizierung und symmetrischen Verschlüsselungsschlüsseln.

- [TLS-Protokoll \(Transport Layer Security\)](#)
- [Datagramm-TLS-Protokoll \(Transport Layer Security\)](#)

Siehe auch

[Windows-Authentifizierung](#) [Kerberos-Authentifizierung](#)

TLS-Protokoll (Transport Layer Security)

09.04.2020 • 6 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows 10

In diesem Thema für IT-Experten wird beschrieben, wie das Transport Layer Security (TLS)-Protokoll funktioniert und Links zu den IETF-RFCs für TLS 1,0, TLS 1,1 und TLS 1,2 bereitstellt.

Die TLS-(und SSL-) Protokolle befinden sich zwischen der Anwendungsprotokoll Ebene und der TCP/IP-Schicht, wo Sie Anwendungsdaten sichern und an die Transportschicht senden können. Da die Protokolle zwischen der Anwendungsschicht und der Transportschicht funktionieren, können TLS und SSL mehrere Protokolle auf Anwendungsebene unterstützen.

TLS und SSL nehmen an, dass ein Verbindungs orientierter Transport (in der Regel TCP) verwendet wird. Das Protokoll ermöglicht Client-und Server Anwendungen, die folgenden Sicherheitsrisiken zu erkennen:

- Manipulation von Nachrichten
- Abfangen der Nachricht
- Nachrichten Fälschung

Die TLS-und SSL-Protokolle können in zwei Ebenen unterteilt werden. Die erste Ebene besteht aus dem Anwendungsprotokoll und den drei Hand Shake-Protokollen: dem Handshake-Protokoll, dem Änderungs Verschlüsselungsprotokoll und dem Warnungs Protokoll. Die zweite Ebene ist das Daten Satz Protokoll. In der folgenden Abbildung werden die verschiedenen Ebenen und ihre Elemente veranschaulicht.

TLS-und SSL-Protokoll Ebenen

Der Schannel-SSP implementiert die TLS-und SSL-Protokolle ohne Änderungen. Das SSL-Protokoll ist proprietär, aber die Internet Engineering Task Force erstellt die öffentlichen TLS-Spezifikationen. Informationen dazu, welche TLS-oder SSL-Version in Windows-Versionen unterstützt wird, finden Sie unter [Protokolle in TLS/SSL \(Schannel SSP\)](#). In der folgenden Tabelle sind die Spezifikationen für jede TLS-Version aufgeführt. Jede Spezifikation enthält Informationen zu folgenden Informationen:

- Das TLS-Daten Satz Protokoll
- Die TLS-handlerprotokolle: - Änderungsprotokoll für Protokoll - Warnungs Protokoll
- Kryptografische Berechnungen
- Obligatorische Verschlüsselungs Sammlungen
- Anwendungsdaten Protokoll

[RFC 5246-die Transport Layer Security \(TLS\)-Protokoll Version 1,2](#)

[RFC 4346-die Transport Layer Security \(TLS\)-Protokoll Version 1,1](#)

[RFC 2246-TLS-Protokoll, Version 1,0](#)

TLS-Sitzungs Wiederaufnahme

Der Schannel SSP wurde in Windows Server 2012 R2 eingeführt und implementierte den Server seitigen Teil der Wiederaufnahme der TLS-Sitzung. Die Client seitige Implementierung von RFC 5077 wurde in Windows 8

hinzugefügt.

Geräte, die TLS-Verbindungen mit Servern herstellen, müssen die Verbindung häufig wiederherstellen. Durch die Wiederaufnahme der TLS-Sitzung werden die Kosten für das Einrichten von TLS-Verbindungen reduziert, da die Wiederaufnahme einen Dadurch wird eine größere Anzahl von Wiederholungsversuchen ermöglicht, da eine Gruppe von TLS-Servern die TLS-Sitzungen der anderen Gruppe wieder aufnehmen kann. Diese Änderung bietet die folgenden Einsparungen für jeden TLS-Client, der RFC 5077 unterstützt, einschließlich Windows Phone und Windows RT-Geräten:

- Reduzierter Ressourcenbedarf auf dem Server
- Reduzierte Bandbreite und damit verbesserte Effizienz von Clientverbindungen
- Reduzierte Zeit für den TLS-Handshake aufgrund von Fortlaufen der Verbindung

Informationen zur Zustandslosen Wiederaufnahme der TLS-Sitzung finden Sie im IETF-Dokument [RFC 5077](#).

Anwendungsprotokoll Aushandlung

In Windows Server 2012 R2 und Windows 8.1 wurde Unterstützung eingeführt, die die Clientseitige TLS-Anwendungsprotokoll Aushandlung ermöglicht. Anwendungen können Protokolle als Teil der http 2,0-Standardentwicklung nutzen, und Benutzer können auf Onlinedienste z. B. Google und Twitter zugreifen, indem Sie Apps verwenden, die das SPDY-Protokoll ausführen.

Weitere Informationen zur Funktionsweise der Anwendungsprotokoll Aushandlung finden Sie unter [Transport Layer Security \(TLS\) Application Layer Protocol Aushandlungs Erweiterung](#).

TLS-Unterstützung für Servernamensanzeige-Erweiterungen

Das SNI-Feature stellt eine Erweiterung der Protokolle SSL und TLS dar und ermöglicht die richtige Identifizierung des Servers, wenn zahlreiche virtuelle Abbilder auf einem einzelnen Server ausgeführt werden. In einem virtuellen Hostingszenario werden mehrere Domänen (die jeweils über ein eigenes potenziell unterschiedliches Zertifikat verfügen) auf einem Server gehostet. In diesem Fall kann der Server nicht im Voraus wissen, welches Zertifikat an den Client gesendet werden soll. SNI ermöglicht es dem Client, die Zieldomäne weiter oben im Protokoll zu informieren. Dies ermöglicht es dem Server, das richtige Zertifikat ordnungsgemäß auszuwählen.

Die folgende zusätzliche Funktionalität:

- Ermöglicht das Hosten mehrerer SSL-Websites in einer einzelnen Internet Protokoll- und Port Kombination.
- Der Speicherbedarf wird reduziert, wenn mehrere SSL-Websites auf einem einzelnen Webserver gehostet werden.
- Ermöglicht mehr Benutzern das gleichzeitige Herstellen von Verbindungen mit SSL-Websites

Datagramm-TLS-Protokoll (Transport Layer Security)

09.04.2020 • 2 minutes to read • [Edit Online](#)

Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows 10

In diesem Referenz Thema für IT-Experten wird das DTLS-Protokoll (Datagram Transport Layer Security) beschrieben, das Teil des SChannel Security Support Provider (SSP) ist.

Das DTLS-Protokoll, das im SChannel SSP in Windows Server 2012 und Windows 8 eingeführt wurde, bietet Kommunikationsdaten Schutz für Datagramm-Protokolle. Informationen dazu, welche DTLS-Version in Windows-Versionen unterstützt wird, finden Sie unter [Protokolle in TLS/SSL \(SChannel SSP\)](#). Das Protokoll ermöglicht Client- und Serveranwendungen, so zu kommunizieren, dass Lauschangriffe, Manipulationen oder Nachrichtenfälschung verhindert werden. Das DTLS-Protokoll basiert auf dem Transport Layer Security-Protokoll (TLS) und bietet gleichwertige Sicherheitsgarantien. Dies mindert die Notwendigkeit, IPsec zu verwenden oder ein benutzerdefiniertes Sicherheitsprotokoll für die Anwendungsschicht zu entwerfen.

Datagramme sind häufig in Streamingmedien, z. b. Spiele oder gesicherte Videokonferenzen. Entwickler können Anwendungen entwickeln, um das DTLS-Protokoll im Kontext des SSPI-Modells (Security Support Provider Interface) der Windows-Authentifizierung zu verwenden, um die Kommunikation zwischen Clients und Servern zu sichern. Das DTLS-Protokoll basiert auf dem User Datagram-Protokoll (UDP). DTLS ist so konzipiert, dass es so ähnlich wie möglich ist, um die neue Sicherheits Erfindung zu minimieren und den Umfang der Code-und Infrastruktur Wiederverwendung zu maximieren.

Die Verschlüsselungs Sammlungen, die für die Konfiguration verfügbar sind, werden nach den für die Konfiguration konfigurierten Verschlüsselungs Sammlungen gemustert. RC4 ist nicht zulässig. SChannel verwendet weiterhin Cryptography Next Generation (CNG). Dadurch wird die in Windows Vista eingeführte in Windows Vista eingeführte PPS 140-Zertifizierung genutzt.

Siehe auch

[IETF RFC 4347 Datagram Transport Layer Security](#)

So funktioniert die Benutzerkontosteuerung

09.04.2020 • 30 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Mithilfe der Benutzerkontensteuerung (User Account Control, UAC) können Computer gegen Schäden durch Schadsoftware (auch als "Malware" bezeichnet) geschützt werden, sodass Organisationen besser verwaltete Desktops bereitstellen können. Dank UAC werden Anwendungen und Aufgaben immer im Sicherheitskontext eines Kontos ohne Administratorberechtigungen ausgeführt, es sei denn, ein Administrator autorisiert gezielt Administratorzugriff zum System. UAC kann die automatische Installation nicht autorisierter Anwendungen blockieren und unbeabsichtigte Änderungen an den Systemeinstellungen verhindern.

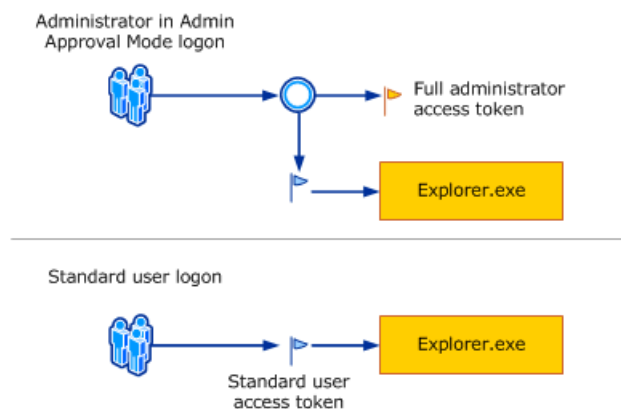
UAC-Prozess und Interaktionen

Jede Anwendung, die das Administrator Zugriffs Token erfordert, muss den Administrator zur Zustimmung auffordern. Die einzige Ausnahme ist die Beziehung, die zwischen den über- und den untergeordneten Prozessen besteht. Untergeordnete Prozesse erben das Benutzer Zugriffs Token vom übergeordneten Prozess. Allerdings müssen sowohl die über- als auch die untergeordneten Prozesse die gleiche Integritätsebene besitzen. Windows Server 2012 schützt Prozesse durch Markieren Ihrer Integritäts Ebenen. Integritätsebenen geben Aufschluss über die Vertrauenswürdigkeit. Eine Anwendung mit „hoher“ Integrität führt Aufgaben aus, die Systemdaten ändern, beispielsweise eine Anwendung für die Datenträgerpartitionierung. Demgegenüber führt eine Anwendung mit „niedriger“ Integrität Aufgaben aus, die das Betriebssystem potenziell gefährden könnten, beispielsweise ein Webbrowser. Anwendungen mit niedrigeren Integritäts Stufen können Daten in Anwendungen mit höheren Integritäts Stufen nicht ändern. Wenn ein Standardbenutzer versucht, eine Anwendung auszuführen, die ein Administrator Zugriffs Token erfordert, erfordert UAC, dass der Benutzer gültige Administrator Anmelde Informationen bereitstellt.

Um besser zu verstehen, wie dieser Prozess passiert, ist es wichtig, die Details zum Anmeldevorgang von Windows Server 2012 zu überprüfen.

Windows Server 2012-Anmeldevorgang

In der folgenden Abbildung wird veranschaulicht, wie sich der Anmeldevorgang für einen Administrator vom Anmeldevorgang für einen Standardbenutzer unterscheidet.



Standardmäßig greifen Standardbenutzer und Administratoren auf Ressourcen zu und führen Anwendungen im Sicherheitskontext von Standardbenutzern aus. Wenn sich ein Benutzer an einem Computer anmeldet, erstellt das System einen Zugriffstoken für diesen Benutzer. Das Zugriffstoken beinhaltet Informationen zu den Zugriffsrechten, die dem Benutzer zustehen, einschließlich der Sicherheits-IDs und der Windows-Berechtigungen.

Wenn sich ein Administrator anmeldet, werden für den Benutzer zwei separate Zugriffstoken erstellt: ein Zugriffstoken für Standardbenutzer und ein Zugriffstoken für Administratoren. Das Standardbenutzer-Zugriffstoken enthält dieselben benutzerspezifischen Informationen wie das Administratorzugriffstoken, die Windows-Administratorberechtigungen und SIDs wurden hierbei jedoch entfernt. Das Standardbenutzer Zugriff Token wird verwendet, um Anwendungen zu starten, die keine administrativen Aufgaben ausführen (Standardbenutzer Anwendungen). Das Standardbenutzer Zugriffs Token wird dann verwendet, um den Desktop (Explorer.exe) anzuzeigen. "Explorer.exe" ist der übergeordnete Prozess, von dem alle anderen vom Benutzer initiierten Prozesse ihre Zugriffstoken erben. Daher werden alle Anwendungen mit Standardbenutzerrechten ausgeführt, sofern ein Benutzer nicht seine Zustimmung erklärt oder seine Anmeldeinformationen angibt, um einer Anwendung die Verwendung eines vollständigen Administratorzugriffstokens zu gestatten.

Ein Benutzer, der Mitglied der Gruppe Administratoren ist, kann sich mit einem Zugriffstoken für Standardbenutzer anmelden, im Internet surfen und E-Mails lesen. Wenn der Administrator einen Task ausführen muss, für den das Administrator Zugriff Token erforderlich ist, wird der Benutzer von Windows Server 2012 automatisch zur Genehmigung aufgefordert. Diese Eingabeaufforderung wird als Eingabeaufforderung für erhöhte Rechte bezeichnet, und das Verhalten kann mithilfe des Snap-Ins für die lokale Sicherheitsrichtlinie (Secpol.msc) oder der Gruppenrichtlinie konfiguriert werden.

NOTE

Der Begriff "Elevate" wird verwendet, um auf den Prozess in Windows Server 2012 zu verweisen, der den Benutzer zur Zustimmung oder zur Eingabe von Anmelde Informationen auffordert, um ein Token für den vollen Administrator Zugriff zu verwenden.

Die UAC-Benutzeroberfläche

Wenn UAC aktiviert ist, unterscheidet sich die Benutzeroberfläche für Standardbenutzer von der für Administratoren im Administratorgenehmigungsmodus. Die empfohlene und sicherere Methode zum Ausführen von Windows Server 2012 besteht darin, Ihr primäres Benutzerkonto als Standardbenutzer Konto zu erstellen. Bei der Ausführung als Standardbenutzer wird die Sicherheit für eine verwaltete Umgebung maximiert. Mit der integrierten UAC-Komponente für erhöhte Rechte können Standardbenutzer einfach eine Verwaltungsaufgabe ausführen, indem sie die gültigen Anmeldeinformationen für ein lokales Administratorkonto eingeben. Bei der standardmäßigen integrierten UAC-Komponente für erhöhte Rechte für Standardbenutzer handelt es sich um die Administratoranmeldeaufforderung.

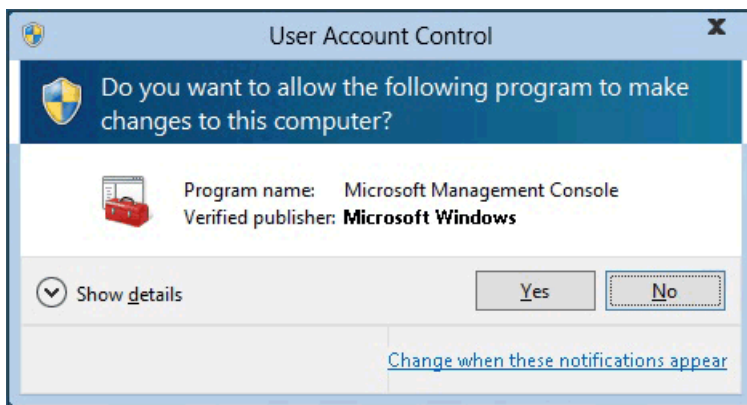
Die Alternative zur Ausführung als ein Standardbenutzer besteht in der Ausführung als ein Administrator im Administratorgenehmigungsmodus. Mit der integrierten Benutzerkontensteuerungs-Komponente für die Höherstufung von Rechten können Mitglieder der lokalen Gruppe Administratoren durch Erteilen einer Genehmigung problemlos eine administrative Aufgabe ausführen. Die standardmäßige integrierte UAC-Komponente für erhöhte Rechte für ein Administratorkonto im Administratorgenehmigungsmodus wird als Zustimmungsaufforderung bezeichnet. Das UAC-Eingabe Aufforderungs Verhalten für erhöhte Rechte kann mithilfe des Snap-Ins "lokale Sicherheitsrichtlinie" (secpol.msc) oder Gruppenrichtlinie konfiguriert werden.

Die Eingabe Aufforderungen für Zustimmung und Anmelde Informationen

Wenn UAC aktiviert ist, werden Sie von Windows Server 2012 zur Zustimmung aufgefordert, oder Sie werden zur Eingabe von Anmelde Informationen eines gültigen lokalen Administrator Kontos aufgefordert, bevor ein Programm oder eine Aufgabe gestartet wird, für die ein vollständiges Administrator Durch diese Aufforderung wird sichergestellt, dass keine Schadsoftware automatisch installiert wird.

Die Zustimmungsaufforderung

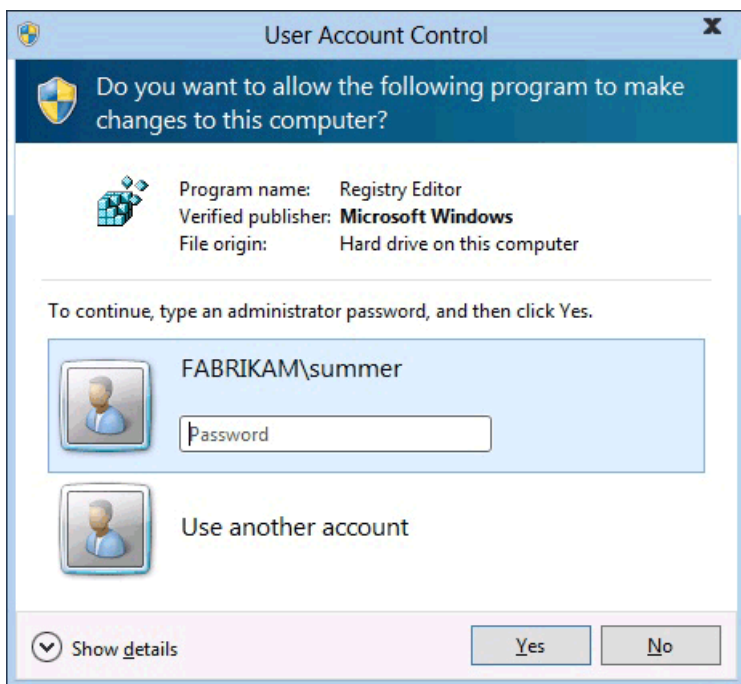
Die Zustimmungsaufforderung wird angezeigt, wenn ein Benutzer versucht, eine Aufgabe auszuführen, für die das Verwaltungszugriffstoken eines Benutzers erforderlich ist. Im folgenden sehen Sie einen Screenshot der UAC-Zustimmungsaufforderung.



Die Administratoranmeldeanforderung

Die Administratoranmeldeanforderung wird angezeigt, wenn ein Standardbenutzer eine Aufgabe ausführen möchte, für die das Administratorzugriffstoken erforderlich ist. Dieses standardmäßige Eingabeaufforderungsverhalten für Standardbenutzer kann mithilfe des Snap-Ins der lokalen Sicherheitsrichtlinie (Secpol.msc) oder der Gruppenrichtlinie konfiguriert werden. Administratoren können auch zur Angabe ihrer Anmeldeinformationen aufgefordert werden, indem der Richtlinieneinstellungswert Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus auf Eingabeaufforderung zu Anmeldeinformationen festgelegt wird.

Der folgende Screenshot zeigt ein Beispiel für die UAC-Eingabeaufforderung für Anmelde Informationen.



UAC-Eingabe Aufforderungen

Die Eingabeaufforderungen für erhöhte Rechte in der Benutzerkontensteuerung besitzen eine Farbcodierung, damit sie bestimmten Anwendungen zugeordnet werden können. Dadurch wird die direkte Identifizierung der potenziellen Sicherheitsrisiken einer Anwendung ermöglicht. Wenn eine Anwendung versucht, mit dem vollständigen Zugriffs Token eines Administrators auszuführen, analysiert Windows Server 2012 zunächst die ausführbare Datei, um deren Verleger zu ermitteln. Anwendungen werden zuerst basierend auf dem Verleger der ausführbaren Datei in drei Kategorien unterteilt: Windows Server 2012, Publisher verifiziert (signiert) und Publisher nicht verifiziert (unsigned). Im folgenden Diagramm wird veranschaulicht, wie Windows Server 2012 die Eingabeaufforderung für die Erhöhung von Farben für den Benutzer festlegt.

Die Farbcodierung für die Eingabeaufforderung für erhöhte Rechte lautet wie folgt:

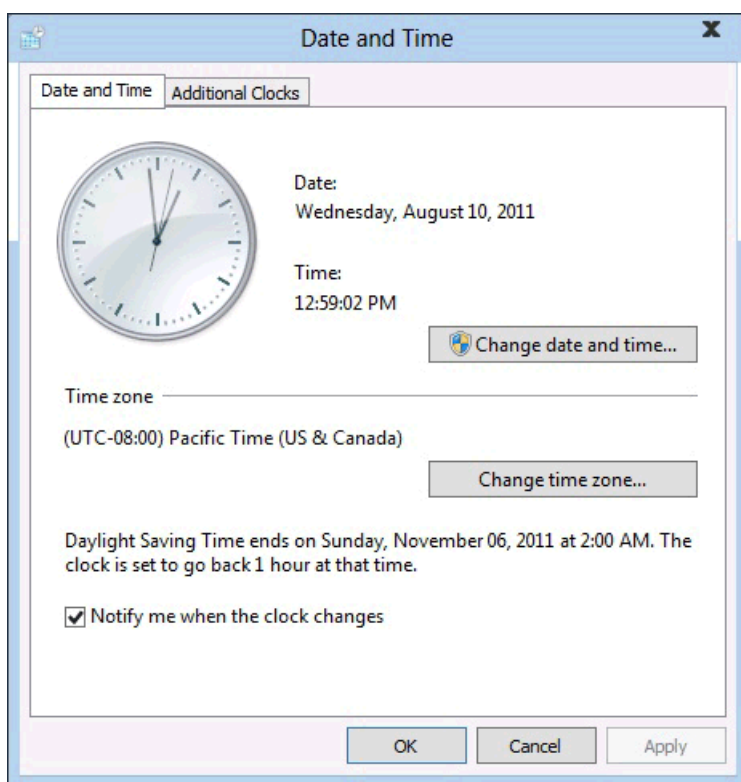
- Roter Hintergrund mit einem roten Schildsymbol: Die Anwendung wird von der Gruppenrichtlinie gesperrt,

oder sie stammt von einem gesperrten Herausgeber.

- Blauer Hintergrund mit einem blauen und goldenen Schild Symbol: die Anwendung ist eine Windows Server 2012-Verwaltungs Anwendung, z. b. ein System Steuerungselement.
- Blauer Hintergrund mit blauem Schildsymbol: Die Anwendung wird mithilfe von Authenticode signiert und wird vom lokalen Computer als vertrauenswürdig eingestuft.
- Gelber Hintergrund mit gelbem Schildsymbol: Die Anwendung ist nicht signiert oder signiert, doch sie wird vom lokalen Computer nicht als vertrauenswürdig eingestuft.

Schild Symbol

Einige Optionen in der Systemsteuerung, zum Beispiel **Datums- und Uhrzeiteigenschaften**, enthalten eine Kombination aus Administrator- und Standardbenutzervorgängen. Standardbenutzer können die Uhrzeit anzeigen und die Zeitzone ändern, doch zum Ändern der lokalen Systemzeit ist ein Token für vollständigen Administratorzugriff erforderlich. Nachfolgend finden Sie einen Screenshot der Systemsteuerungsoption **Datums- und Uhrzeiteigenschaften**.



Das Schildsymbol auf der Schaltfläche **Datum und Uhrzeit ändern** gibt an, dass der Prozess ein Token für vollständigen Administratoren erfordert. Eine Eingabeaufforderung für erhöhte Rechte der Benutzerkontensteuerung wird angezeigt.

Sichern der Eingabeaufforderung für erhöhte Rechte

Die Höherstufung von Rechten wird zusätzlich durch Weiterleiten der Aufforderung an den sicheren Desktop gesichert. Die Eingabeaufforderungen für Zustimmung und Anmeldeinformationen werden standardmäßig auf dem sicheren Desktop unter Windows Server 2012 angezeigt. Nur Windows-Prozesse können auf den sicheren Desktop zugreifen. Ein höheres Sicherheitsniveau erzielen Sie, wenn Sie die Richtlinieneinstellung **Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln** aktiviert lassen.

Wenn eine ausführbare Datei erhöhte Rechte erfordert, wechselt der interaktive Desktop (wird auch als Benutzerdesktop bezeichnet) zum sicheren Desktop. Der sichere Desktop blendet den Benutzerdesktop ab und zeigt eine Eingabeaufforderung für erhöhte Rechte an, die beantwortet werden muss, bevor der Vorgang fortgesetzt werden kann. Wenn der Benutzer auf Ja oder Nein klickt, wechselt der Desktop wieder zurück zum

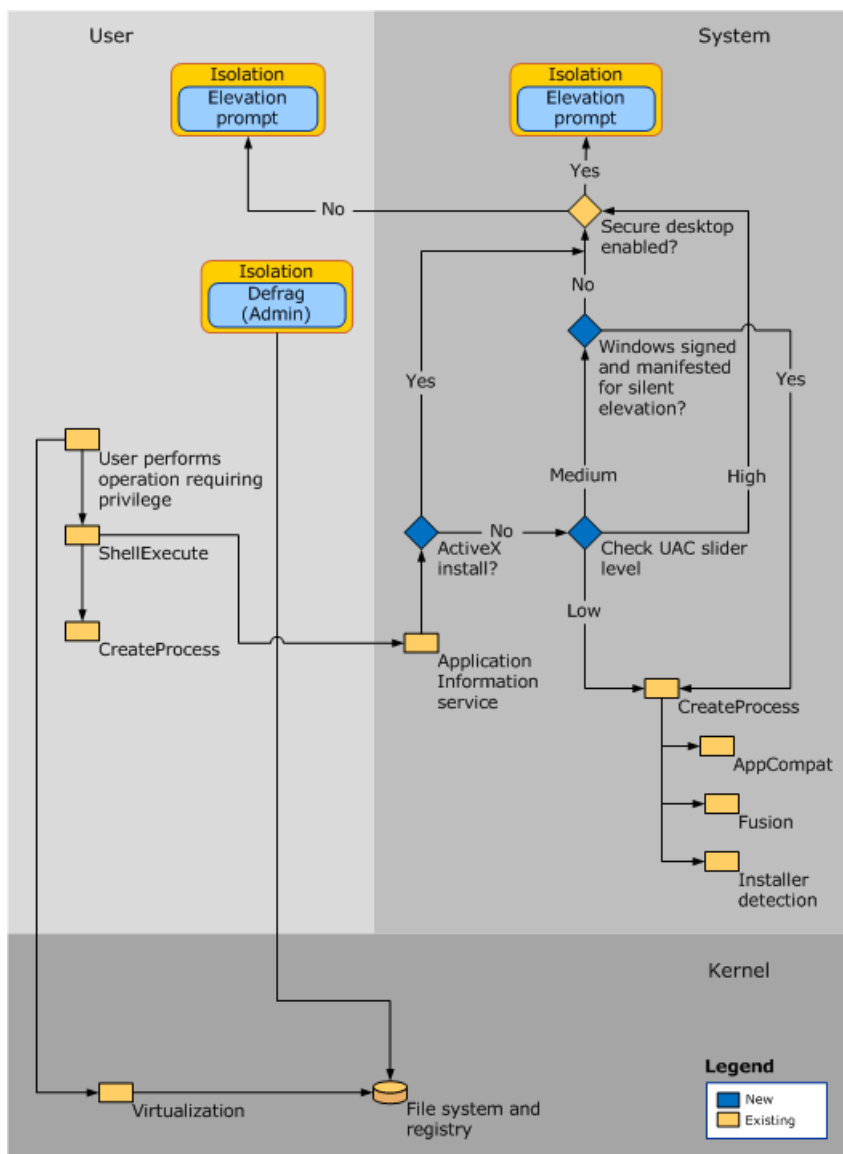
Benutzerdesktop.

Schadsoftware kann eine Imitation des sicheren Desktops darstellen, doch wenn die Richtlinieneinstellung Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus auf Eingabeaufforderung zur Zustimmung festgelegt wurde, erhält die Schadsoftware keine erhöhten Rechte, wenn der Benutzer auf dem imitierten Desktop auf Ja klickt. Wenn die Richtlinieneinstellung auf Eingabeaufforderung zu Anmeldeinformationen festgelegt wird, kann Schadsoftware, die die Administratoranmeldeanforderung imitiert, möglicherweise die Anmeldeinformationen des Benutzers sammeln. Die Schadsoftware erhält jedoch keine erhöhten Rechte, und das System weist andere Schutzmechanismen auf, die verhindern, dass die Schadsoftware die Steuerung der Benutzeroberfläche übernimmt, selbst wenn das Kennwort abgeleitet wird.

Auch wenn Schadsoftware eine Imitation des sicheren Desktops darstellen kann, kann dieses Problem nur dann auftreten, wenn ein Benutzer die Schadsoftware zuvor auf dem Computer installiert hat. Da Prozesse, für die ein Administratorzugriffstoken erforderlich ist, nicht unbeaufsichtigt installiert werden können, wenn die Benutzerkontensteuerung aktiviert ist, muss der Benutzer ausdrücklich seine Zustimmung erklären, indem er auf **Ja** klickt oder Administratoranmeldeinformationen angibt. Die spezifische Verhaltensweise der UAC-Eingabeaufforderung für erhöhte Rechte hängt von „Gruppenrichtlinie“ ab.

UAC-Architektur

Im folgenden Diagramm wird die UAC-Architektur (Architektur der Benutzerkontensteuerung) detailliert dargestellt.



Überprüfen Sie die folgende Tabelle, um die einzelnen Komponenten besser zu verstehen:

| KOMPONENTE | BESCHREIBUNG |
|--|---|
| User | |
| Benutzer führt einen Vorgang aus, für den eine Berechtigung erforderlich ist | Wenn bei dem Vorgang das Dateisystem oder die Registrierung geändert wird, wird die Virtualisierung aufgerufen. Bei allen anderen Vorgängen wird ShellExecute aufgerufen. |
| ShellExecute | ShellExecute ruft CreateProcess auf. ShellExecute sucht nach dem Fehler "ERROR_ELEVATION_REQUIRED" von CreateProcess. Wenn der Fehler empfangen wird, ruft ShellExecute den Anwendungsinformationsdienst auf, um die angeforderte Aufgabe mit der Eingabeaufforderung für erhöhte Rechte auszuführen. |
| CreateProcess | Wenn für die Anwendung eine Erhöhung erforderlich ist, lehnt "kcreateprocess" den-Befehl mit ERROR_ELEVATION_REQUIRED ab. |
| Anlage | |
| Anwendungsinformationsdienst | Ein Systemdienst, der den Start von Anwendungen unterstützt, die zur Ausführung mindestens ein erhöhtes Recht oder Benutzerrecht benötigen (zum Beispiel lokale administrative Aufgaben), sowie von Anwendungen, die höhere Integritätsebenen erfordern. Der Anwendungs Informationsdienst hilft dabei, solche Anwendungen zu starten, indem er einen neuen Prozess für die Anwendung mit dem vollständigen Zugriffs Token eines Administrators erstellt, wenn eine Erhöhung erforderlich ist und (je nach Gruppenrichtlinie) Zustimmung vom Benutzer erteilt wird. |
| Erhöhen einer ActiveX-Installation | Wenn ActiveX nicht installiert ist, überprüft das System die UAC-Schiebereglerstufe. Wenn ActiveX installiert ist, wird die Gruppenrichtlinieneinstellung Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln aktiviert. |

| KOMPONENTE | BESCHREIBUNG |
|---|--|
| Stufe des UAC-Schiebereglers überprüfen | <p>UAC verfügt jetzt über vier Benachrichtigungs Ebenen, die Sie auswählen können, und einen Schieberegler, mit dem die Benachrichtigungs Ebene ausgewählt wird:</p> <ul style="list-style-type: none"> • Hoch
Wenn der Schieberegler auf Immer benachrichtigen gerichtet ist, wird vom System überprüft, ob der sichere Desktop aktiviert ist. • Mittel
Wenn der Schieberegler auf Standard - nur benachrichtigen, wenn Änderungen am Computer von Programmen vorgenommen werden gerichtet ist, ist die Richtlinieneinstellung Benutzerkontensteuerung: Nur ausführbare Dateien heraufstufen, die signiert und überprüft sind aktiviert: <ul style="list-style-type: none"> ◦ Wenn die Richtlinien Einstellung aktiviert ist, wird die Überprüfung der PKI-Zertifizierungs Pfade (Public Key-Infrastruktur) für eine bestimmte ausführbare Datei erzwungen, bevor Sie ausgeführt werden darf. ◦ Wenn die Richtlinieneinstellung nicht aktiviert ist (Standard), wird die Überprüfung des Public Key-Infrastrukturzertifizierungspfads erst erzwungen, wenn eine angegebene ausführbare Datei ausgeführt werden darf. Die Gruppenrichtlinieneinstellung Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln ist aktiviert. • Niedrig
Wenn der Schieberegler auf Nur benachrichtigen, wenn Änderungen am Computer von Programmen vorgenommen werden (Desktop nicht abblenden) gerichtet ist, wird CreateProcess aufgerufen. • Nie benachrichtigen
Wenn der Schieberegler auf "nie Benachrichtigen" festgelegt ist, wird die UAC-Eingabeaufforderung nie benachrichtigt, wenn ein Programm versucht, eine Änderung auf dem Computer zu installieren oder zu versuchen, eine Änderung vorzunehmen. Wichtig: Diese Einstellung wird nicht empfohlen. Diese Einstellung entspricht dem Festlegen der Richtlinieneinstellung Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorgenehmigungsmodus auf Erhöhte Rechte ohne Eingabeaufforderung. |

| KOMPONENTE | BESCHREIBUNG |
|-------------------------------|--|
| Aktivierter sicherer Desktop | <p>Die Richtlinieneinstellung Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln ist aktiviert:</p> <p>-Wenn der sichere Desktop aktiviert ist, werden alle Anforderungen für erhöhte Rechte unabhängig von den Richtlinien Einstellungen für das Eingabe Aufforderungs Verhalten für Administratoren und Standardbenutzer an den sicheren Desktop gesendet.</p> <p>Wenn der sichere Desktop nicht aktiviert ist, werden alle Anforderungen für erhöhte Rechte an den Desktop des interaktiven Benutzers gesendet, und die benutzerspezifischen Einstellungen für Administratoren und Standardbenutzer werden verwendet.</p> |
| CreateProcess | <p>Von "anateprocess" werden AppCompat-, Fusion-und Installer-Erkennung aufgerufen, um zu bewerten, ob die Anwendung eine Erhöhung Die ausführbare Datei wird anschließend überprüft, um die angeforderte Ausführungsebene zu bestimmen, die im Anwendungsmanifest der ausführbaren Datei gespeichert ist. CreateProcess schlägt fehl, wenn die im Manifest angegebene angeforderte Ausführungsebene nicht dem Zugriffstoken entspricht. In diesem Fall wird ein Fehler (ERROR_ELEVATION_REQUIRED) an ShellExecute zurückgegeben.</p> |
| AppCompat | <p>Die AppCompat-Datenbank speichert Informationen in den Anwendungskompatibilitätspatch-Einträgen für eine Anwendung.</p> |
| Fusion | <p>In der Fusion-Datenbank werden Informationen aus dem Anwendungsmanifesten gespeichert, die die Anwendungen beschreiben. Das Manifestschema wird aktualisiert, um ein Feld für das Hinzufügen einer neuen angeforderten Ausführungsstufe hinzuzufügen.</p> |
| Installationserkennung | <p>Die Installationsprogramm Erkennung erkennt ausführbare Setup Dateien, um zu verhindern, dass Installationen ohne Kenntnis und Zustimmung des Benutzers ausgeführt werden.</p> |
| - | |
| Virtualisierung | <p>Virtualisierungstechnologie stellt sicher, dass nicht kompatible Anwendungen nicht im Hintergrund ausgeführt werden oder fehlschlagen, wenn die Ursache nicht ermittelt werden kann. UAC bietet zudem eine Datei- und Registrierungsvirtualisierung und Protokollierung für Anwendungen, die in geschützte Bereiche schreiben.</p> |
| Dateisystem und Registrierung | <p>Die benutzerbasierte Datei- und Registrierungsvirtualisierung leitet die Schreibanforderung für die computerbasierte Registrierung und Datei an die entsprechenden benutzerbasierten Speicherorte um. Leseanforderungen werden zuerst an den virtualisierten Einzelbenutzerort und anschließend an den Einzelcomputerort umgeleitet.</p> |

In früheren Windows-Versionen gibt es eine Änderung an Windows Server 2012 UAC. Der neue Schieberegler

schaltet die UAC niemals vollständig aus. Die neue Einstellung sieht wie folgt aus:

- Der UAC-Dienst wird weiterhin ausgeführt.
- Alle durch Administratoren initiierten Eingabeaufforderungen für erhöhte Rechte werden automatisch genehmigt, ohne dass eine UAC-Eingabeaufforderung angezeigt wird.
- Für Standardbenutzer werden automatisch alle Eingabeaufforderungen für erhöhte Rechte abgelehnt.

IMPORTANT

Zum vollständigen Deaktivieren von UAC müssen Sie die Richtlinie **Benutzerkontensteuerung: Alle Administratoren im Administratorgenehmigungsmodus ausführen** deaktivieren.

WARNING

Angepasste Anwendungen können unter Windows Server 2012 nicht verwendet werden, wenn UAC deaktiviert ist.

Virtualisierung

Da Systemadministratoren in Unternehmensumgebungen Systeme sichern möchten, sind zahlreiche Branchenanwendungen so konzipiert, dass nur ein Zugriffstoken für Standardbenutzer verwendet wird. Dies hat zur Folge, dass IT-Administratoren beim Ausführen von Windows Server 2012 mit aktivierter UAC nicht die Mehrzahl der Anwendungen ersetzen müssen.

Windows Server 2012 umfasst die Datei- und Registrierungsvirtualisierungstechnologie für Anwendungen, die nicht UAC-kompatibel sind und für die ein Administrator Zugriffstoken erforderlich ist. Durch die Virtualisierung wird sichergestellt, dass selbst Anwendungen, die nicht UAC-kompatibel sind, mit Windows Server 2012 kompatibel sind. Wenn eine administrative Anwendung, die nicht UAC-kompatibel ist, versucht, in ein geschütztes Verzeichnis (z. B. Programmdateien) zu schreiben, gibt die UAC der Anwendung eine eigene virtualisierte Ansicht der Ressource, die Sie zu ändern versucht. Die virtualisierte Kopie wird im Profil des Benutzers verwaltet. Diese Strategie erstellt eine separate Kopie der virtualisierten Datei für jeden Benutzer, der die nicht kompatible Anwendung ausführt.

Die meisten Anwendungsaufgaben werden ordnungsgemäß mithilfe von Virtualisierungsfeatures ausgeführt. Auch wenn die Virtualisierung die Ausführung der meisten Anwendungen zulässt, handelt es sich hierbei um einen kurzfristigen Patch und nicht um eine langfristige Lösung. Anwendungsentwickler sollten Ihre Anwendungen so schnell wie möglich so ändern, dass Sie mit dem Windows Server 2012-Logo Programm kompatibel sind, anstatt sich auf die Virtualisierung von Dateien, Ordnern und Registrierungen verlassen zu müssen.

Virtualisierung ist in den folgenden Szenarien keine Option:

1. Die Virtualisierung gilt nicht für Anwendungen mit erhöhten Rechten, die mit einem vollen Administrator Zugriffstoken ausgeführt werden.
2. Virtualisierung unterstützt nur 32-Bit-Anwendungen. 64-Bit-Anwendungen ohne erhöhte Rechte erhalten einfach eine Meldung vom Typ "Zugriff verweigert", wenn Sie versuchen, ein Handle (einen eindeutigen Bezeichner) für ein Windows-Objekt abzurufen. Native Windows 64-Bit-Anwendungen müssen mit UAC kompatibel sein und Daten an die richtigen Speicherorte schreiben.
3. Die Virtualisierung ist für eine Anwendung deaktiviert, wenn die Anwendung ein Anwendungs Manifest mit einem angeforderten Attribut auf Ausführungsebene enthält.

Anforderungs Ausführungsebenen

Ein Anwendungsmanifest ist eine XML-Datei, die die freigegebenen und privaten parallelen Assemblys, mit denen eine Anwendung eine Bindung erstellen soll, beschreibt und identifiziert. In Windows Server 2012 enthält das

Anwendungs Manifest Einträge für die UAC-Anwendungs Kompatibilität. Administrative Anwendungen, die einen Eintrag im Anwendungs Manifest enthalten, fordern den Benutzer zur Eingabe der Berechtigung für den Zugriff auf das Zugriffs Token des Benutzers auf. Obwohl ihnen ein Eintrag im Anwendungsmanifest fehlt, können die meisten Administratoranwendungen ohne Änderung ausgeführt werden, indem Anwendungskompatibilitätspatches verwendet werden. Anwendungskompatibilitäts-Fixes sind Datenbankeinträge, mit denen Anwendungen, die nicht UAC-kompatibel sind, ordnungsgemäß mit Windows Server 2012 funktionieren.

Allen UAC-kompatiblen Anwendungen muss eine angeforderte Ausführungs Ebene hinzugefügt werden, die dem Anwendungs Manifest hinzugefügt wurde. Wenn die Anwendung Administrator Zugriff auf das System erfordert, stellt das Markieren der Anwendung mit der angeforderten Ausführungs Ebene "Administrator erforderlich" sicher, dass das System dieses Programm als administrative Anwendung identifiziert, und führt die erforderlichen Schritte zur Erhöhung der Rechte aus. Die angeforderten Ausführungsebenen geben die für eine Anwendung erforderlichen Rechte an.

Installer-Erkennungstechnologie

Installationsprogramme sind Anwendungen, die zur Bereitstellung von Software entwickelt wurden. Die meisten Installationsprogramme schreiben Daten in Systemverzeichnisse und Registrierungsschlüssel. In diese geschützten Systemspeicherorte kann für gewöhnlich nur ein Administrator oder die Technologie für Installationserkennung schreiben. Somit verfügt ein Standardbenutzer nicht über den benötigten Zugriff, um Programme zu installieren. Windows Server 2012 heuristisch erkennt Installationsprogramme und fordert Administrator Anmelde Informationen oder eine Genehmigung vom Administrator Benutzer an, um mit Zugriffsberechtigungen ausgeführt zu werden. Windows Server 2012 erkennt auch heuristisch Updates und Programme, mit denen Anwendungen deinstalliert werden. Eines der Entwurfsziele für die Benutzerkontensteuerung besteht darin, zu verhindern, dass Installationen ohne das Wissen und die Zustimmung des Benutzers ausgeführt werden, da Installationsprogramme Schreibvorgänge in geschützten Bereichen des Dateisystems und der Registrierung ausführen.

Die Installationserkennung gilt für:

- Ausführbare 32-Bit-Dateien.
- Anwendungen ohne Attribut für die angeforderte Ausführungsebene.
- Interaktive Prozesse, die mit aktivierter UAC als ein Standardbenutzer ausgeführt werden.

Vor dem Erstellen eines 32-Bit-Prozesses werden die folgenden Attribute überprüft, um zu ermitteln, ob sie sich in einem Installer befinden:

- Der Dateiname enthält Schlüsselwörter wie „install“, „setup“ oder „update“.
- Felder für Versionsverwaltungsressourcen enthalten die folgenden Schlüsselwörter: Anbieter, Unternehmensname, Produktname, Dateibeschriftung, Ursprünglicher Dateiname, Interner Name und Exportname.
- Schlüsselwörter im parallelen Manifest werden in die ausführbare Datei eingebettet.
- Schlüsselwörter in spezifischen „StringTable“-Einträgen werden in der ausführbaren Datei verknüpft.
- Wichtige Attribute in den Ressourcenskriptdaten werden in der ausführbaren Datei verknüpft.
- In der ausführbaren Datei befinden sich Zielbytesequenzen.

NOTE

Die Schlüsselwörter und Bytesequenzen sind an allgemeine Merkmale angelehnt, die auch in verschiedenen Installationstechnologien zu finden sind.

NOTE

Die Richtlinieneinstellung Benutzerkontensteuerung: Anwendungsinstallationen erkennen und erhöhte Rechte anfordern muss für die Installationserkennung aktiviert werden, damit Installationsprogramme erkannt werden. Diese Einstellung wird standardmäßig aktiviert und kann lokal mithilfe des Snap-Ins für die lokale Sicherheitsrichtlinie (Secpol.msc) oder für die Domäne, OE oder für bestimmte Gruppen nach Gruppenrichtlinie (Gpedit.msc) konfiguriert werden.

Einführen der tokenbindung

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016 und Windows 10

Das tokenbindungsprotokoll ermöglicht Anwendungen und Diensten das kryptografische binden ihrer Sicherheits Token an die TLS-Schicht, um tokendiebstahl und Replay-Angriffe zu verhindern Die langlebige, eindeutig identifizierbaren TLS-Bindungen [RFC5246] können mehrere TLS-Sitzungen und-Verbindungen umfassen.

Versions Unterstützung:

- Windows 10, Version 1507 – standardmäßig deaktiviert
 - Tokenbindungsprotokoll hinzugefügt [\[Draft-IETF-tokbind-Protocol-01\]](#)
 - WinInet & http. SYS-Unterstützung der [tokenbindung über http](#) [\[Draft-IETF-tokbind-HTTPS-01\]](#)
- Windows 10, Version 1511 und 1607 und Windows Server 2016 – standardmäßig aktiviert
 - Tokenbindungsprotokoll aktualisiert [\[Draft-IETF-tokbind-Protocol-01\]](#)
 - TLS-Erweiterung für [tokenbindungs-Aushandlung](#) hinzugefügt [\[Draft-Popov-tokbind-Aushandlung-00\]](#)
 - WinInet & http. SYS-Unterstützung der [tokenbindung über HTTP](#) aktualisiert [\[Draft-IETF-tokbind-HTTPS-02\]](#)
- Windows 10, Version 1507 mit Wartungsupdate [KB4034668](#), Windows 10, Version 1511 mit Wartungsupdate [KB4034660](#), Windows 10, Version 1607 und Windows Server 2016 mit Wartungsupdate [KB4034658](#) Support Token Binding Protocol Version 0,10 – on default
 - Tokenbindungsprotokoll aktualisiert [\[Draft-IETF-tokbind-Protocol-10\]](#)
 - TLS-Erweiterung für [tokenbindungs-Aushandlung](#) hinzugefügt [\[Draft-IETF-tokbind-Aushandlung-05\]](#)
 - WinInet & http. SYS-Unterstützung der [tokenbindung über HTTP](#) aktualisiert [\[Draft-IETF-tokbind-HTTPS-06\]](#)
- Windows 10, Version 1703 unterstützt das tokenbindungsprotokoll Version 0,10 – standardmäßig on
 - Tokenbindungsprotokoll aktualisiert [\[Draft-IETF-tokbind-Protocol-10\]](#)
 - TLS-Erweiterung für [tokenbindungs-Aushandlung](#) hinzugefügt [\[Draft-IETF-tokbind-Aushandlung-05\]](#)
 - WinInet & http. SYS-Unterstützung der [tokenbindung über HTTP](#) aktualisiert [\[Draft-IETF-tokbind-HTTPS-06\]](#)
 - Bei Windows-Geräten mit aktivierter virtualisierungsbasierter Sicherheit werden die tokenbindungsschlüssel in einer geschützten Umgebung aufbewahrt, die vom laufenden Betriebssystem isoliert ist.

Informationen zur ASP .NET-Unterstützung finden Sie im [.NET Framework Verweis Quelle](#).

Weitere Informationen zu .NET Framework finden Sie in den folgenden Themen:

- [Netzwerk Erweiterungen](#)
- [.Net tokenbinding-Klasse](#)

Windows Defender Antivirus für Windows Server

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

Windows Server 2016 enthält jetzt Windows Defender Antivirus. Windows Defender AV ist ein Malware Schutz, der Windows Server 2016 sofort und aktiv vor bekannten Schadsoftware schützt und die antischadsoftwaredefinitionen regelmäßig über Windows Update aktualisieren kann.

Weitere Informationen finden Sie in der Dokumentationsbibliothek zu [Windows Defender Antivirus in Windows 10](#).

Obwohl die Funktionalität, Konfiguration und Verwaltung von Windows Defender AV auf Windows 10 oder Windows Server 2016 größtenteils identisch ist, gibt es einige wichtige Unterschiede:

- In Windows Server 2016 werden basierend auf Ihrer definierten Serverrolle [automatische Ausschlüsse](#) angewendet.
- In Windows Server 2016 deaktiviert Windows Defender AV sich nicht selbst, wenn Sie ein anderes Antivirenprodukt ausführen.

Das Thema [Windows Defender Antivirus unter Windows Server 2016](#) enthält Informationen zu den Informationen zu Windows Server 2016, einschließlich der folgenden:

- [Aktivieren der Schnittstelle](#)
- [Überprüfen, ob Windows Defender AV ausgeführt wird](#)
- [Antischadsoftwaredefinitionen aktualisieren](#)
- [Absenden von Beispielen](#)
- [Automatische Ausschlüsse konfigurieren](#)