Anwenderadministration

Virtual Desktop Service

NetApp
February 20, 2023

Inhaltsverzeichnis

Anwenderadministration

Verwalten Von Benutzerkonten

Neuen Benutzer erstellen

Administratoren können Benutzer hinzufügen, indem sie auf Arbeitsbereiche > Benutzer und Gruppen > Hinzufügen/Importieren klicken

Benutzer können einzeln oder mit einem Massenimport hinzugefügt werden.

[Breite = 25 %]

> Einschließlich genauer E-Mail und Handy # in dieser Phase verbessert den Prozess der Aktivierung MFA später erheblich.

Sobald Sie Benutzer erstellt haben, können Sie auf ihren Namen klicken, um Details zu sehen, wie wann sie erstellt wurden, ihren Verbindungsstatus (ob sie gerade angemeldet sind oder nicht) und was ihre spezifischen Einstellungen sind.

Aktivieren des Virtual Desktop für vorhandene AD-Benutzer

Wenn Benutzer bereits in AD vorhanden sind, können Sie den Virtual Desktop der Benutzer einfach aktivieren, indem Sie auf das System neben ihrem Namen klicken und dann ihren Desktop aktivieren.[Breite = 50 %]

> Nur für den Azure AD-Domänendienst: Damit die Anmeldung funktioniert, muss der Password-Hash für Azure AD-Benutzer synchronisiert werden, um die NTLM- und Kerberos-Authentifizierung zu unterstützen. Am einfachsten ist es, das Benutzerpasswort in Office.com oder im Azure Portal zu ändern, sodass die Hash-Synchronisierung des Passworts erzwungen wird. Der Synchronisierungszyklus für Domain Service-Server kann bis zu 20 Minuten dauern, sodass Änderungen an Passwörtern in Azure AD in der Regel 20 Minuten in AADDS und damit in der VDS-Umgebung wieder aufnehmen können.

Benutzerkonto(e) löschen

Benutzerinformationen bearbeiten

Auf der Benutzerdetailseite können Änderungen an den Benutzerdetails wie Benutzername und Kontaktdaten vorgenommen werden. Die E-Mail- und Telefonwerte werden für den SSPR-Prozess (Self Service Password Reset) verwendet.

[]

Sicherheitseinstellungen für Benutzer bearbeiten

- VDI-Benutzer aktiviert – eine RDS-Einstellung, die, wenn sie aktiviert ist, einen dedizierten VM-Session-Host erstellt und diesem Benutzer als einzigen Benutzer zugewiesen wird, der eine Verbindung zu ihm herstellt. Im Rahmen der Aktivierung dieses Kontrollkästchens wird der CWMS-Administrator aufgefordert, VM-Image, -Größe und -Speichertyp auszuwählen.
    - AVD-VDI-Benutzer sollten auf der AVD-Seite als VDI-Hostpool verwaltet werden.

- Kontoablauf aktiviert – ermöglicht dem CWMS-Administrator, ein Ablaufdatum auf dem Endbenutzerkonto festzulegen.
- Passwort zurücksetzen bei der nächsten Anmeldung erzwingen – fordert den Endbenutzer auf, sein Passwort bei der nächsten Anmeldung zu ändern.
- Multi-Faktor Auth aktiviert – aktiviert MFA für den Endbenutzer und fordert ihn zur Einrichtung von MFA bei der nächsten Anmeldung auf.
- Mobile Drive Enabled – eine ältere Funktion, die in aktuellen RDS- oder AVD-Bereitstellungen nicht verwendet wird.
- Lokaler Laufwerkszugriff aktiviert – ermöglicht es dem Endbenutzer, von der Cloud-Umgebung aus auf den lokalen Gerätebsspeicher zuzugreifen, einschließlich Kopieren/Einfügen, USB-Massenspeicher und Systemlaufwerke.
- Wake-on-Demand aktiviert – für RDS-Benutzer, die sich über den CW-Client für Windows verbinden, erhalten sie dadurch die Berechtigung, ihre Umgebung zu nehmen, wenn sie außerhalb der normalen Arbeitszeiten gemäß Workload Schedule eine Verbindung herstellen.

Gesperrtes Konto

Standardmäßig sperren fünf fehlgeschlagene Anmeldeversuche das Benutzerkonto. Das Benutzerkonto wird nach 30 Minuten entsperrt, es sei denn, *Enable Password Komplexitäts* ist aktiviert. Wenn die Passwortkomplexität aktiviert ist, wird das Konto nicht automatisch entsperrt. In beiden Fällen kann der VDS-Administrator das Benutzerkonto manuell von der Seite Benutzer/Gruppen im VDS entsperren.

Benutzerpasswort zurücksetzen

Setzt das Benutzerpasswort zurück.

Hinweis: Beim Zurücksetzen von Azure AD-Benutzerpasswörtern (oder beim Entsperren eines Kontos) kann es eine Verzögerung von bis zu 20 Minuten geben, wenn das Zurücksetzen über Azure AD propagiert.

Administratorzugriff

Wenn dies ermöglicht wird, erhält der Endbenutzer eingeschränkten Zugriff auf das Management-Portal für seinen Mandanten. Zu den üblichen Nutzungsmöglichkeiten gehört die Bereitstellung eines vor-Ort-Mitarbeiters, der auf das Zurücksetzen von Peers-Passwörtern, die Zuweisung von Anwendungen oder das Zulassen von manuellen Server-Wakeup-Zugriffen zugreifen kann. Berechtigungen, die steuern, welche Bereiche der Konsole angezeigt werden können, werden auch hier festgelegt.

Benutzer abmelden

Angemeldete Benutzer können vom VDS-Administrator von der Seite Benutzer/Gruppen im VDS abgemeldet werden.

Applikationen Unterstützt

Zeigt die in diesem Arbeitsbereich bereitgestellte Anwendung an. Das Kontrollkästchen stellt die Apps für diesen spezifischen Benutzer bereit. Vollständige Dokumentation zum Application Management finden Sie hier. Der Zugriff auf Anwendungen kann auch über die App-Schnittstelle oder auf Security Groups gewährt werden.

Benutzerprozesse anzeigen/beenden

Zeigt die Prozesse an, die derzeit in der Sitzung des Benutzers ausgeführt werden. Auch von dieser Schnittstelle können Prozesse beendet werden.

Managen Von Datenberechtigungen

Aus der Sicht des Endbenutzers

Endbenutzer von virtuellen Desktops können auf mehrere zugeordnete Laufwerke zugreifen. Zu diesen Laufwerken zählen eine auf FTA zugängliche Teamfreigabe, eine Company File Share und ihr Home Drive (für Dokumente, Desktop usw.…). . Alle diese zugeordneten Laufwerke verweisen auf eine zentrale Storage-Ebene entweder auf ein Storage-Service (z. B. Azure NetApp Files) oder auf einer File Server-VM.

Je nach Konfiguration des Benutzers kann der Benutzer nicht über die Laufwerke H: Oder F: Freigelegt haben, können sie nur ihren Desktop, Dokumente, etc… sehen Ordner. Darüber hinaus werden gelegentlich bei der Bereitstellung verschiedene Laufwerksbuchstaben vom VDS-Administrator festgelegt.[]

[]

Verwalten von Berechtigungen

MIT VDS können Administratoren Sicherheitsgruppen und Ordnerberechtigungen über das VDS-Portal bearbeiten.

Sicherheitsgruppen

Sicherheitsgruppen werden verwaltet, indem Sie im Abschnitt Gruppen auf Workspaces > Mandantenname > Benutzer & Gruppen > klicken

In diesem Abschnitt können Sie:

1. Erstellen Sie neue Sicherheitsgruppen
2. Benutzer zu den Gruppen hinzufügen/entfernen
3. Anwendungen Gruppen zuweisen
4. Aktivieren/Deaktivieren des Zugriffs auf lokale Laufwerke für Gruppen

[]

Ordnerberechtigungen

Ordnerberechtigungen werden verwaltet, indem Sie auf Workspaces > Mandantenname > Verwalten klicken (im Abschnitt Ordner).

In diesem Abschnitt können Sie:

1. Ordner Hinzufügen/Löschen
2. Weisen Sie Benutzern oder Gruppen Berechtigungen zu
3. Passen Sie die Berechtigungen an schreibgeschützt, vollständige Kontrolle und Keine an

[]

Applikationsberechtigung

Überblick

VDS verfügt über eine robuste integrierte Anwendungsautomatisierung und Berechtigungsfunktionalität. Mit dieser Funktion können Benutzer auf verschiedene Anwendungen zugreifen, während eine Verbindung zu demselben Sitzungshost(s) hergestellt wird. Dies wird durch einige benutzerdefinierte GPOs, die Verknüpfungen ausblenden zusammen mit der Automatisierung selektiv platziert Verknüpfungen auf den Desktops der Benutzer.

Dieser Workflow gilt nur für RDS-Implementierungen. Informationen zu AVD-Anwendungsberechtigungen finden Sie unter "Anwendungsberechtigungsworkflow für AVD"

Anwendungen können Benutzern direkt oder über in VDS gemanagte Sicherheitsgruppen zugewiesen werden.

Im allgemeinen folgt der Bereitstellungsprozess von Applikationen diesen Schritten.

1. App(s) zum App-Katalog hinzufügen
2. Fügen Sie dem Arbeitsbereich App(s) hinzu
3. Installieren Sie die Anwendung auf allen Sitzungshosts
4. Wählen Sie den Verknüpfungspfad aus
5. Weisen Sie Benutzern und/oder Gruppen Apps zu

Die Schritte 3 und 4 können wie unten dargestellt vollständig automatisiert werden

Video-Präsentation

Fügen Sie Anwendungen zum App-Katalog hinzu

VDS-Anwendungsberechtigung beginnt mit dem App-Katalog. Dies ist eine Liste aller Anwendungen, die für die Bereitstellung in Endbenutzerumgebungen zur Verfügung stehen.

Führen Sie die folgenden Schritte aus, um dem Katalog Anwendungen hinzuzufügen

1. Melden Sie sich bei VDS an https://manage.cloudworkspace.com Verwendung der primären Anmeldedaten des Administrators
2. Klicken Sie oben rechts auf das Pfeilsymbol neben Ihrem Benutzernamen und wählen Sie Einstellungen aus.
3. Klicken Sie auf die Registerkarte App Catalog.
4. Klicken Sie in der Titelleiste des Anwendungskatalogs auf die Option App hinzufügen.
5. Um eine Gruppe von Anwendungen hinzuzufügen, wählen Sie die Option Apps importieren.
    a. Es wird ein Dialogfeld angezeigt, in dem eine Excel-Vorlage zum Herunterladen angezeigt wird, die das richtige Format für die Anwendungsliste erzeugt.
    b. Für diese Bewertung hat NetApp VDS eine Beispiel-Applikationsliste für den Import erstellt. Diese finden Sie hier.
    c. Klicken Sie auf den Bereich Hochladen und wählen Sie die Datei mit der Anwendungsvorlage aus. Klicken Sie auf die Schaltfläche Importieren.
6. Wenn Sie einzelne Anwendungen hinzufügen möchten, wählen Sie die Schaltfläche App hinzufügen, und es wird ein Dialogfeld angezeigt.
    a. Geben Sie den Namen der Anwendung ein.
    b. Mit einer externen ID kann eine interne Tracking-ID eingegeben werden, z. B. eine Produkt-SKU oder ein Abrechnungsverfolgungscode (optional).
    c. Aktivieren Sie das Kontrollkästchen Abonnement, wenn Sie über die Anwendungen als Abonnementprodukt berichten möchten (optional).
    d. Wenn das Produkt nicht nach Version installiert wird (z. B. Chrome), aktivieren Sie das Kontrollkästchen Version nicht erforderlich. So können Produkte mit kontinuierlicher Aktualisierung installiert werden, ohne ihre Versionen nachzuverfolgen.
    e. Wenn ein Produkt mehrere benannte Versionen unterstützt (z. B. QuickBooks), müssen Sie dieses Kontrollkästchen aktivieren, damit Sie mehrere Versionen installieren und jede verfügbare Version in der Liste der Anwendungen, die für und Endbenutzer berechtigt sein können, VDS-spezifisch besitzen können.
    f. Aktivieren Sie „kein Benutzer-Desktop-Symbol“, wenn VDS kein Desktop-Symbol für dieses Produkt bereitstellen soll. Dies wird für „Backend“-Produkte wie SQL Server verwendet, da Endbenutzer keine Anwendung haben, auf die sie zugreifen können.
    g. „App muss zugeordnet sein“ setzt die Notwendigkeit, eine zugehörige App zu installieren. Für eine Client-Server-Anwendung kann es z. B. erforderlich sein, dass auch SQL Server oder MySQL installiert werden muss.
    h. Wenn Sie das Feld Lizenz erforderlich aktivieren, wird angezeigt, dass VDS eine Lizenzdatei für eine Installation dieser Anwendung anfordern sollte, bevor der Anwendungsstatus auf aktiv gesetzt wird. Dieser Schritt wird auf der Seite Anwendungsdetails von VDS durchgeführt.
    i. Sichtbar für Alle – Anwendungsberechtigungen können auf bestimmte Teilpartner in einer Mehrkanalhierarchie beschränkt werden. Klicken Sie zu Evaluierungszwecken auf das Kontrollkästchen, damit alle Benutzer es in ihrer Liste der verfügbaren Anwendungen sehen können.

Fügen Sie die Anwendung dem Arbeitsbereich hinzu

Um den Bereitstellungsprozess zu starten, fügen Sie die App zum Arbeitsbereich hinzu.

Führen Sie dazu die folgenden Schritte aus

1. Klicken Sie Auf Arbeitsbereiche
2. Blättern Sie nach unten zu „Apps“
3. Klicken Sie Auf Hinzufügen
4. Aktivieren Sie die Anwendung(en), geben Sie die erforderlichen Informationen ein, klicken Sie auf Anwendung hinzufügen und klicken Sie auf Apps hinzufügen.

Installieren Sie die Anwendung manuell

Sobald die Anwendung dem Arbeitsbereich hinzugefügt wurde, müssen Sie diese Anwendung auf allen Sitzungshosts installieren. Dies kann manuell und/oder automatisiert werden.

Führen Sie die folgenden Schritte aus, um Anwendungen manuell auf Sitzungshosts zu installieren

1. Navigieren Sie zu Service Board.
2. Klicken Sie auf die Aufgabe des Service Board.
3. Klicken Sie auf die Servernamen, um eine Verbindung als lokaler Administrator herzustellen.
4. Installieren Sie die App(s), bestätigen Sie, dass die Verknüpfung zu dieser Anwendung im Startmenü-Pfad gefunden wird.
    a. Für Server 2016 und Windows 10: C:\ProgramData\Microsoft\Windows\Startmenü\Programme.
5. Gehen Sie zurück zur Aufgabe des Service-Mainboards, klicken Sie auf Durchsuchen und wählen Sie entweder die Verknüpfung oder einen Ordner mit Verknüpfungen aus.
6. Je nachdem, welche Option Sie auswählen, wird auf dem Desktop des Endbenutzers angezeigt, wenn die App zugewiesen wurde.
7. Ordner sind großartig, wenn eine Anwendung tatsächlich mehrere Anwendungen ist. Z. B. „Microsoft Office“ ist einfacher als Ordner mit jeder App als Verknüpfung im Ordner bereitzustellen.
8. Klicken Sie Auf Installation Abschließen.
9. Öffnen Sie bei Bedarf das erstellte Symbol Serviceboard Task hinzufügen, und bestätigen Sie, dass das Symbol hinzugefügt wurde.

Anwendungen zu Benutzern zuweisen

Die Anwendungsberechtigungen werden von VDS verwaltet, und die Anwendung kann Benutzern auf drei Arten zugewiesen werden

Anwendungen zu Benutzern zuweisen

1. Navigieren Sie zur Seite „Benutzerdetails“.
2. Navigieren Sie zum Abschnitt Anwendungen.
3. Aktivieren Sie das Kontrollkästchen neben allen für diesen Benutzer erforderlichen Anwendungen.

Weisen Sie einer Anwendung Benutzer zu

1. Navigieren Sie auf der Seite Arbeitsbereichdetails zum Abschnitt Anwendungen.
2. Klicken Sie auf den Namen der Anwendung.

3. Aktivieren Sie das Kontrollkästchen neben den Benutzern, die die Anwendung verwenden.

Anwendungen und Benutzer zu Benutzergruppen zuweisen

1. Navigieren Sie zu den Benutzern und Gruppen-Details.
2. Fügen Sie eine neue Gruppe hinzu oder bearbeiten Sie eine vorhandene Gruppe.
3. Weisen Sie der Gruppe Benutzer und Anwendungen zu.

Benutzerpasswort Zurücksetzen

Schritte für das Benutzerpasswort zurücksetzen

1. Navigieren Sie zur Seite „verwendete Details“ im VDS

   []

2. Suchen Sie den Abschnitt Kennwort, geben Sie zweimal den neuen PW ein, und klicken Sie auf

   []

   []

Zeit, um wirksam zu werden

- Für Umgebungen, die ein „internes“ AD auf VMs in der Umgebung ausführen, sollte die Passwortänderung sofort wirksam werden.
- In Umgebungen, in denen Azure AD Domain Services (AADDS) ausgeführt wird, sollte die Passwortänderung ca. 20 Minuten in Anspruch nehmen.
- Der AD-Typ kann auf der Seite „Bereitstellungsdetails“ ermittelt werden:

  []

Self Service password Reset (SSRP)

Der NetApp VDS Windows-Client und der NetApp VDS Web-Client erhalten eine Eingabeaufforderung für Benutzer, die bei der Anmeldung bei einer Virtual Desktop-Implementierung mit v5.2 (oder höher) ein falsches Passwort eingeben. Falls der Benutzer sein Konto gesperrt hat, wird dieser Prozess auch das Konto eines Benutzers entsperren.

Hinweis: Benutzer müssen bereits eine Mobiltelefonnummer oder eine E-Mail-Adresse eingegeben haben, damit dieser Prozess funktioniert.

SSPR wird unterstützt durch:

- NetApp VDS Window Client
- NetApp VDS Web Client

In diesem Satz von Anweisungen werden Sie den Prozess der Verwendung von SSPR als einfache Mittel, um Benutzern zu ermöglichen, ihre Passwörter zurückzusetzen und ihre Konten zu entsperren.

NetApp VDS Windows-Client

1. Klicken Sie als Endbenutzer auf den Link Passwort vergessen, um fortzufahren.

   []

2. Wählen Sie aus, ob Sie Ihren Code über Ihr Mobiltelefon oder per E-Mail erhalten möchten.

   []

3. Wenn ein Endbenutzer nur eine dieser Kontaktmethoden bereitgestellt hat, wird dies die einzige Methode angezeigt.

   []

4. Nach diesem Schritt wird den Benutzern ein Code-Feld angezeigt, in dem sie den Wert eingeben, der entweder auf ihrem Mobilgerät oder in ihrem Posteingang empfangen wurde (je nachdem, welcher Wert ausgewählt wurde). Geben Sie diesen Code gefolgt vom neuen Passwort ein und klicken Sie auf Zurücksetzen, um fortzufahren.

   []

5. Der Benutzer wird aufgefordert, ihn darüber zu informieren, dass das Zurücksetzen des Passworts erfolgreich abgeschlossen wurde. Klicken Sie auf „Fertig“, um den Anmeldevorgang abzuschließen.

   > Wenn Ihre Bereitstellung Azure Active Directory Domain Services verwendet, gibt es einen von Microsoft definierten Zeitraum zur Kennwortsynchronisation – alle 20 Minuten. Auch dies wird von Microsoft gesteuert und kann nicht geändert werden. In diesem Sinne zeigt VDS an, dass der Benutzer bis zu 20 Minuten warten sollte, bis sein neues Passwort wirksam wird. Wenn Ihre Bereitstellung Azure Active Directory Domain Services nicht verwendet, kann sich der Benutzer in Sekundenschnelle erneut anmelden.

   []

HTML5-Portal

1. Wenn der Benutzer beim Versuch, sich über den HTML5 anzumelden, das richtige Passwort nicht eingibt, wird ihm nun eine Option zum Zurücksetzen des Passworts angezeigt:

   []

2. Nachdem Sie auf die Option zum Zurücksetzen des Passworts geklickt haben, werden ihnen die Optionen zum Zurücksetzen angezeigt:

   []

3. Die Schaltfläche ‘Anfrage’ sendet einen generierten Code an die ausgewählte Option (in diesem Fall die E-Mail des Benutzers). Der Code ist 15 Minuten lang gültig.

   []

4. Das Kennwort wurde zurückgesetzt! Es ist wichtig zu beachten, dass Windows Active Directory häufig einen Moment benötigt, um die Änderung zu verbreiten. Wenn das neue Passwort also nicht sofort funktioniert, warten Sie einfach ein paar Minuten und versuchen Sie es erneut. Dies ist insbesondere für Benutzer mit Azure Active Directory Domain Services-Implementierung relevant, wobei das Zurücksetzen

des Passworts bis zu 20 Minuten dauern kann.

[]

Aktivieren des Self-Service-Kennwortrücksetzens (SSPR) für Benutzer

Um Self Service Password Reset (SSPR) zu verwenden, müssen Administratoren zunächst eine Handynummer und/oder ein E-Mail-Konto für einen Endbenutzer eingeben. Es gibt zwei Möglichkeiten, wie unten beschrieben eine Handynummer und E-Mail-Adressen für einen virtuellen Desktop-Benutzer einzugeben.

In diesem Satz von Anweisungen werden Sie den Prozess der Konfiguration von SSPR als einfache Möglichkeit für Endbenutzer, ihre Passwörter zurückzusetzen, durchlaufen.

Massenimport von Benutzern über VDS

Navigieren Sie zunächst zum Workspaces-Modul, dann zu Benutzern & Gruppen und klicken Sie dann auf Hinzufügen/Importieren.

Sie können die folgenden Werte für Benutzer eingeben, wenn Sie sie einzeln erstellen:[]

Oder Sie können diese einschließen, wenn Benutzer im Massenimport die vorkonfigurierte Excel XLSX-Datei herunterladen und mit diesem Inhalt hochladen:[]

Bereitstellen der Daten über die VDS-API

NetApp VDS API – insbesondere dieser Aufruf https://api.cloudworkspace.com/5.4/swagger/ui/index#!/User/User_PutUser – Bietet die Möglichkeit, diese Informationen zu aktualisieren.

Das vorhandene Benutzertelefon wird aktualisiert

Aktualisieren Sie die Telefonnummer der Benutzer auf der Seite „Übersicht der Benutzerdetails“ im VDS.

[]

Verwenden anderer Konsolen

Hinweis: Es ist derzeit nicht möglich, eine Telefonnummer für einen Benutzer über die Azure Console, das Partner Center oder über die Office 365 Admin-Konsole bereitzustellen.

SSPR-Sendeadresse anpassen

NetApp VDS kann so konfiguriert werden, dass er die Bestätigungs-E-Mail *von* einer benutzerdefinierten Adresse sendet. Dies ist ein Service für unsere Service Provider-Partner, die ihre Endbenutzer möchten, dass sie die Reset-Passwort-E-Mail von ihrer eigenen angepassten E-Mail-Domäne erhalten.

Diese Anpassung erfordert einige weitere Schritte, um die Absendeadresse zu überprüfen. Um diesen Prozess zu starten, öffnen Sie einen Support-Fall mit VDS-Unterstützung und fordern eine benutzerdefinierte „Self Service Password Reset Source Address“ an. Bitte definieren Sie Folgendes:

- Ihr Partner-Code (dieser Code kann durch Klicken auf *settings* unter dem oberen rechten Pfeil nach unten Menü gefunden werden. Siehe Abbildung unten)

  []

- Gewünschte „von“-Adresse (gültig)
- Auf welche Clients die Einstellung angewendet werden soll (oder alle)

Die Eröffnung eines Support Cases kann per E-Mail an support@spotpc.netapp.com erfolgen

Sobald VDS-Unterstützung erhalten ist, wird die Adresse mit unserem SMTP-Dienst validiert und diese Einstellung aktiviert. Idealerweise haben Sie die Möglichkeit, öffentliche DNS-Datensätze in der Quelladdress Domain zu aktualisieren, um die Zustellung von E-Mails zu maximieren.

Komplexität von Passwörtern

VDS kann so konfiguriert werden, dass die Passwortkomplexität durchgesetzt wird. Die Einstellung hierzu finden Sie auf der Seite Arbeitsbereichdetails im Abschnitt Einstellungen des Cloud-Arbeitsbereichs.

[]

[]

Passwortkomplexität: Aus

Richtlinie	Richtlinie
Mindestkennwortlänge	8 Zeichen
Maximales Kennwortalter	110 Tage
Mindestalter Des Kennworts	0 Tage
Kennwortverlauf Erzwingen	24 Passwörter gespeichert
Passwort Sperren	Nach 5 falschen Einträgen erfolgt die automatische Sperrung
Sperrdauer	30 Minuten

Passwortkomplexität: Ein

Richtlinie	Richtlinie
Mindestkennwortlänge	8 Zeichen enthalten nicht den Kontonamen des Benutzers oder Teile des vollständigen Namens des Benutzers, die zwei aufeinanderfolgende Zeichen überschreiten, enthalten Zeichen aus drei der folgenden vier Kategorien: Englische Großbuchstaben (A bis Z) Englische Kleinbuchstaben (A bis z) Basis 10 Ziffern (0 bis 9) nicht-alphabetische Zeichen (z. B. !, €, #, %) Komplexitätsanforderungen werden durchgesetzt, wenn Passwörter geändert oder erstellt werden.
Maximales Kennwortalter	110 Tage
Mindestalter Des Kennworts	0 Tage
Kennwortverlauf Erzwingen	24 Passwörter gespeichert
Passwort Sperren	Nach 5 falschen Einträgen erfolgt die automatische Sperre
Sperrdauer	Bleibt gesperrt, bis der Administrator entsperrt wird

Multi-Faktor-Authentifizierung (MFA)

Überblick

NetApp Virtual Desktop Service (VDS) umfasst ohne Aufpreis einen SMS/E-Mail-basierten MFA Service. Dieser Service ist unabhängig von anderen Dienstleistungen (z.B. Azure Conditional Access) und kann zur Sicherung von Administratoranmeldungen auf VDS und Benutzeranmeldungen auf virtuellen Desktops verwendet werden.

MFA-Grundlagen

- VDS MFA kann Admin-Benutzern, einzelnen Endbenutzern oder für alle Endbenutzer angewendet werden
- VDS MFA kann SMS- oder E-Mail-Benachrichtigungen senden
- VDS MFA verfügt über eine Self-Service-Ersteinrichtung und Reset-Funktion

Umfang des Leitfadens

Dieses Handbuch erläutert die Einrichtung von MFA sowie die Darstellung der Benutzerfreundlichkeit

In diesem Leitfaden werden die folgenden Themen behandelt:

1. MFA für einzelne Benutzer aktivieren
2. MFA für alle Benutzer erforderlich
3. MFA für einzelne Administratoren aktivieren
4. Ersteinrichtung Des Endbenutzers

MFA für einzelne Benutzer aktivieren

MFA kann für einzelne Benutzer auf der Benutzer-Detailseite durch Klicken auf *Multi-Faktor Auth Enabled* aktiviert werden

Arbeitsbereiche > Workspace-Name > Benutzer & Gruppen > Benutzername > Multi-Faktor Auth aktiviert > Aktualisieren

MFA kann auch allen Benutzern zugewiesen werden. Wenn diese Einstellung aktiviert ist, wird das Kontrollkästchen aktiviert und _ (über Client-Einstellungen)_ wird an das Kontrollkästchen angehängt.

MFA für alle Benutzer erforderlich

MFA kann auf der Detailseite des Arbeitsbereichs für alle Benutzer aktiviert und durchgesetzt werden, indem Sie auf *MFA für Alle Benutzer aktiviert* klicken

Workspaces > Workspace-Name > MFA für alle Benutzer aktiviert >Update

Aktivierung von MFA für einzelne Administratoren

MFA ist auch für Administratorkonten verfügbar, die auf das VDS-Portal zugreifen. Dies kann pro Administrator auf der Seite „Administratordetails“ aktiviert werden. Administratoren > Admin-Name > Multi-Faktor-Auth Erforderlich > Aktualisieren

Ersteinrichtung

Bei der ersten Anmeldung nach der Aktivierung von MFA wird der Benutzer oder der Admin aufgefordert, eine E-Mail-Adresse oder Telefonnummer einzugeben. Sie erhalten einen Bestätigungscode, mit dem sie die erfolgreiche Anmeldung bestätigen können.