

NetScaler SDX 14.1

Contents

はじめに	18
リリースノート	19
Management Serviceユーザーインターフェイスの利用を開始する	20
Management Serviceユーザーインターフェイスにログオンする	20
初期設定ウィザード	21
SDXアプライアンスでインスタンスをプロビジョニングする	22
コンソールアクセス	23
Management Serviceの統計	23
Management ServiceおよびNetScalerインスタンスへのシングルサインオン	23
ホームページの管理	23
ポート	25
データガバナンス	26
Console Advisory Connectとは何ですか？	26
NetScaler Consoleサービスとは何ですか？	27
Console Advisory Connectの有効化方法？	27
Console Advisory Connectで取得されるデータ？	27
データの使用方法？	28
収集されたデータの保持期間？	28
データはどこに保存され、どの程度安全ですか？	28
Console Advisory Connectを無効にする方法？	28
NetScaler SDXアプライアンス向けConsole Advisory Connectの概要	29
Console Advisory ConnectはNetScaler Consoleサービスをどのようにサポートするか？	30
Console Advisory ConnectがサポートするNetScalerのバージョン？	30
Console Advisory Connectを有効にする方法？	30
Console Advisory Connectを有効化および無効化する方法？	31
CLIの使用	31

GUIの使用	31
NITRO API の使用	32
NetScaler Console 組み込みエージェントの動作	32
参照	32
シングルバンドルアップグレード	33
NetScaler SDXのアップグレード前の重要な考慮事項	33
必須のバックアップ	33
推定メンテナンス期間	33
段階的なアップグレードパス	34
前提条件	35
注意点	35
アプライアンス全体を 14.1 にアップグレードする	35
サポートされているアップグレードパス	36
関連情報	37
SDX XenServer® 8 へのアップグレード	37
SBI 14.1-47.x 以降でサポートされるNetScalerプラットフォーム	37
SBI 14.1-34.x 以降でサポートされるNetScalerプラットフォーム	37
SBI 14.1-34.x以降でサポートされていないNetScalerプラットフォーム	38
アップグレードマトリックス	38
ダウングレードマトリックス	39
サポートされているVPXバージョン	39
制限事項	40
NetScalerインスタンスのアップグレード	40
ソフトウェアイメージをアップロードするには	41
ビルドファイルをダウンロードしてバックアップを作成するには	41
XVAファイルをアップロードするには	41
XVAファイルをダウンロードしてバックアップを作成するには	42
NetScaler VPXインスタンスのアップグレード	42

VPXインスタンスをアップグレードするには	43
関連情報	43
SDXアプライアンスの管理と監視	44
SDXアプライアンスのネットワーク構成を変更する	44
デフォルトユーザーアカウントのパスワードを変更する	44
アプライアンスのタイムゾーンを変更する	44
アプライアンスのホスト名を変更する	45
VLANフィルタリング	45
クロック同期の構成	46
NTP同期を有効にするには	46
認証オプションを変更するには	46
SDXアプライアンスのプロパティを表示する	47
リアルタイムのアプライアンススループットを表示する	48
リアルタイムのCPUとメモリの使用状況を表示する	48
すべてのコアのCPU使用率を表示する	49
SDXアプライアンスにSSL証明書をインストールする	49
Management ServiceでSSL証明書を表示する	49
NetScalerインスタンス用のSSL証明書とキー	50
システム設定を変更する	50
アプライアンスの再起動	50
アプライアンスのシャットダウン	50
SDX 管理ドメイン	51
サブドメインへのリソース割り当ての例	51
ユーザーをドメインに割り当てる	52
SDX 22000プラットフォームでのRAIDディスク割り当ての管理	53
ドライブのプロパティと操作を表示する	53
論理ドライブ	53
新しい論理ドライブを作成するには	54

物理ドライブ	54
ストレージリポジトリ	55
SDXライセンスの概要	57
ライセンスアクティベーションサービス	58
SDXアプライアンスでのライセンスの管理	58
前提条件	59
Management Service を使用したライセンスの割り当て	59
ライセンスを割り当てるには	59
ライセンスの有効期限とデータトラフィック処理の制限	61
ライセンスアクティベーションサービス	62
LASのNetScalerバージョン互換性	63
前提条件	63
NetScaler GUIを使用したLASへの移行	64
ライセンスアクティベーションファイルの動作と有効期限	66
ライセンス契約の有効期限	67
LASライセンスワークフロー中にLASに送信される情報	67
LAS移行済みNetScaler SDX (SVM) を監視するためのベストプラクティス	69
前提条件	69
LASアクティベーションプロブの有効期限の監視	69
ライセンスエンタイトルメントの有効期限の監視 (契約の有効期限)	71
SDX リソースビジュアライザー	72
インターフェースを管理する	72
インターフェースを構成するには	73
インターフェイスのパラメータをデフォルト値にリセットするには	73
VPXインスタンス上の仮想インターフェイスと物理インターフェイスのマッピングを表示する	73
インターフェイスへのMACアドレスの割り当て	74
SDXアプライアンスの物理インターフェイスを無効または有効にする	75

SDXアプライアンスでのジャンボフレーム	76
ユースケース: ジャンボからジャンボへのセットアップ	77
ユースケース: 非ジャンボからジャンボへのセットアップ	80
ユースケース: 同じインターフェースセット上でのジャンボフローと非ジャンボフローの共存	85
SDXアプライアンスでのSNMPの設定	91
SNMPトラップ宛先を追加するには	92
MIBファイルのダウンロード	92
MIBファイルをダウンロードするには	93
SNMPマネージャーコミュニティの追加	93
SNMPマネージャーを構成するには	93
SNMPv3クエリ用にSDXアプライアンスを構成する	94
SNMPマネージャーの追加	94
SNMPビューの構成	95
ビューを構成するには	95
SNMPユーザーの構成	95
ユーザーを構成するには	95
SNMPアラームの設定	96
Management Serviceインベントリの不一致を監視するためのアラーム	97
syslog通知を設定する	97
syslogサーバーを設定する	98
Syslog パラメータを設定する	98
メール通知の構成	98
SMTPサーバーを構成するには	98
メールプロファイルを構成するには	99
SMS通知を構成する	99
SMSサーバーを構成する	99
SMSプロファイルを構成する	99

SDXアプライアンスに構成されたエンティティのリアルタイムステータスを監視および管理する	100
仮想サーバーのステータスを表示する	100
サービスの状態を表示する	101
サービスグループのステータスを表示する	102
サーバーのステータスを表示する	103
ポーリング間隔を構成する	104
NetScalerインスタンスで生成されたイベントの監視と管理	104
すべてのイベントを表示する	105
イベントを削除する	108
SDXアプライアンス上のNetScalerインスタンスに対するCall Homeサポート	109
システムヘルス監視	111
SDXアプライアンスのストレージリソースを監視する	112
SDXアプライアンスのハードウェアセンサーを監視する	113
SDXアプライアンスのインターフェースを監視する	113
システム通知設定の構成	114
システム通知設定を構成するには	114
Management Service から機能を有効化および無効化する	115
GUI を使用して機能を有効または無効にするには	115
管理サービスを構成する	116
クライアントセッションを管理する	116
管理サービスのメモリを構成する	116
前提条件	117
Management Serviceメモリを構成するには	117
Management Serviceメモリのバックアップと復元	117
ポリシーを構成する	118
Management Serviceを再起動する	119
Management Serviceファイルを削除する	119

テクニカルサポート用のtarアーカイブを生成する	120
Management ServiceのCLIサポート	120
Management ServiceからのBMCアクセスを有効にする	121
管理サービスを使用してLOMアクセスを有効にする	121
認証および承認設定を構成する	122
ユーザーグループを追加する	123
ユーザーグループを追加するには	123
ユーザーアカウントを構成する	124
ユーザーアカウントを構成するには	124
ユーザーアカウントを削除するには	125
認証タイプを設定する	125
認証タイプを設定するには	126
基本認証を有効または無効にする	126
基本認証を無効にするには	126
外部認証サーバーの構成	126
RADIUSサーバーの追加	127
RADIUSサーバーを追加するには	127
LDAP認証サーバーの追加	128
LDAPサーバーを追加するには	128
LDAPユーザーのSSH公開鍵認証サポート	130
FQDN名前解決のためのプライマリDNSの追加	131
TACACSサーバーの追加	131
TACACSサーバーを追加するには	132
Management Serviceからリンクアグリゲーションを構成する	132
Management Service からチャンネルを構成する	133
Management Service からチャンネルを構成するには	134
アクセス制御リスト	135
使用ガイドライン	135

ACLを構成する方法	136
ACL機能を有効にする	136
ACLルールを作成する	136
ACLルールを有効にする	137
ACLルールのその他のアクション	137
ACLルールを無効にする	138
ACLルールを編集する	138
ACLルールを削除する	138
ACLルールの優先順位を振り直す	139
トラブルシューティング	139
NetScalerインスタンスのクラスターをセットアップする	139
留意事項	140
SDXアプライアンスでクラスターをセットアップする	141
あるSDXアプライアンス上に存在するNetScalerインスタンスを、別のSDXアプライアンス上に構成されたクラスターに追加する	144
クラスターリンクアグリゲーションの構成	144
Management Serviceに安全にアクセスするためのSSL暗号の構成	147
制限事項	147
サポートされているSSL暗号	148
事前定義された暗号グループ	154
事前定義された暗号グループを表示する	156
カスタム暗号グループを作成する	156
既存のSSL暗号バインディングを表示する	157
暗号をHTTPSサービスにバインドする	157
SDXアプライアンスの構成データのバックアップと復元	157
現在の構成をバックアップする	158
スケジュールされたバックアップ	158
バックアップポリシーを編集する	158

バックアップファイルを外部バックアップサーバーに手動で転送する	159
バックアップファイルを外部バックアップサーバーに転送する	159
アプライアンスを復元する	159
バックアップファイルからアプライアンスを復元する	160
NetScalerインスタンスをリストアする	162
アプライアンスのリセットを実行する	163
アプライアンスの構成をリセットする	164
アプライアンスの構成をリセット	164
アプライアンスを工場出荷時のバージョンにリセットする	164
アプライアンスを工場出荷時のバージョンにリセットする	165
アプライアンスをシングルバンドルイメージバージョンにリセットする	165
前提条件	166
アプライアンスを単一のバンドルイメージバージョンにリセットする	166
外部認証サーバーのカスケーディング	167
外部認証サーバーをカスケード接続する	167
ユーザーのロックを解除する	167
GUIを使用してユーザーのロックを解除する	168
CLIを使用してユーザーのロックを解除する	168
アドミンプロファイルでnsroot以外のユーザーを作成する	168
SDXでアドミンプロファイル内のnsroot以外のユーザーを使用できるようにする	168
非nsrootユーザーで管理者プロファイルを作成する	169
管理サービスを使用してNetScalerインスタンスを作成する	169
NetScalerインスタンスを編集して、非nsroot管理者プロファイルを割り当てる	169
NetScalerインスタンスにシステムコマンドポリシーをバインドする	170
NetScalerインスタンスで非nsrootユーザーを使用するためのガイドライン	170
NetScalerインスタンスのプロビジョニング	171
管理者プロファイルの作成	172
管理者プロファイルの作成	173

NetScaler .xva イメージをアップロードする	174
NetScaler .xva ファイルをアップロードするには	174
NetScaler .xva ファイルをダウンロードしてバックアップを作成するには	174
NetScaler インスタンスを追加する	175
ライセンス割り当て	175
暗号割り当て	176
リソース割り当て	176
SDX上のNetScaler VPXで追加の管理CPUを有効にするための推奨事項	179
概要	180
追加の管理CPUを有効にするタイミング	181
インスタンス管理	182
ネットワーク設定	182
管理 VLAN 設定	184
NetScaler インスタンスの編集	184
VLANを特定の仮想インターフェースに制限する	185
許可されたVLAN IDを指定するには	186
Management ServiceからインスタンスのVLANを構成するには	186
暗号容量の管理	188
SDX アプライアンスの暗号容量を表示する	189
VPXインスタンスのプロビジョニング中に暗号容量を割り当てる	189
さまざまなSDXアプライアンスで利用可能なACUカウンターの最小値	189
暗号ハードウェアの健全性を表示	190
注意事項	191
ACUからPKEリソースへの変換テーブル	191
ACUからPKEへのリソース変換テーブルの読み方	193
レガシーSSLチップからACUおよびSCUへの変換テーブル	194
サードパーティ製仮想マシンのプロビジョニング	195
SECUREMATRIX GSB	196

SECUREMATRIX GSB インスタンスをプロビジョニングする	196
SECUREMATRIX インスタンスをプロビジョニングするには	197
SECUREMATRIX GSBインスタンスを監視する	198
SECUREMATRIX GSBインスタンスを管理する	198
SECUREMATRIX GSBインスタンスのSDXツールファイルをアップグレードする	198
SECUREMATRIX GSBインスタンスのアップグレードとダウングレード	199
SECUREMATRIX GSB インスタンスのトラブルシューティング	200
トレンドマイクロ InterScan Web Security	201
ウェブセンス プロテクター	202
Websense Protectorインスタンスをプロビジョニングする	203
XVAイメージをSDXアプライアンスにアップロードするには	203
Websense Protectorインスタンスをプロビジョニングするには	203
Websense Protectorインスタンスを監視する	204
Websense Protectorインスタンスを管理する	204
Websense Protectorインスタンスを開始、停止、再起動、強制停止、または強制再起動するには	204
Websense ProtectorインスタンスのSDXツールファイルをアップグレードする	205
SDXツールファイルをアップロードするには	205
SDXツールをアップグレードするには	205
Websense Protectorインスタンスを新しいバージョンにアップグレードする	205
ソフトウェアイメージをアップロードするには	205
インスタンスをアップグレードするには	206
Websense Protectorインスタンスのトラブルシューティング	206
インスタンスにpingを実行するには	206
インスタンスのルートをトレースするには	206
インスタンスを再検出するには	207
BlueCat DNS/DHCP	207
BlueCat DNS/DHCPインスタンスのプロビジョニング	207

BlueCat DNS/DHCPインスタンスの監視	209
BlueCat DNS/DHCP インスタンスの管理	209
BlueCat DNS/DHCP インスタンスの SDXTools ファイルをアップグレードする	210
BlueCat DNS/DHCPインスタンスを再検出する	210
CA アクセス ゲートウェイ	211
CA Access Gatewayインスタンスをプロビジョニングする	211
CA Access Gatewayインスタンスを監視する	212
CA Access Gatewayインスタンスを管理する	213
パロアルトネットワークス VMシリーズ	213
PaloAlto VM-Seriesインスタンスをプロビジョニングする	214
Palo Alto VM-Series インスタンスを監視する	215
PaloAlto VM-Series インスタンスを管理する	215
PaloAlto VM-Seriesインスタンスのトラブルシューティング	215
SDXにおける帯域幅メータリング	217
固定スループットレートの専用帯域幅	217
最小保証スループットと帯域幅バースト機能を備えた専用帯域幅	217
帯域幅割り当てモードの選択	218
VPXインスタンスの最大バースト帯域幅の決定	218
スループットとデータ消費統計の確認	219
NetScalerインスタンスの構成と管理	221
NetScalerインスタンスでSNIPアドレスを作成する	221
NetScalerインスタンスにSNIPアドレスを追加するには	221
構成を保存する	222
NetScalerインスタンスの構成を保存するには	222
NetScalerインスタンスを管理する	222
NetScalerインスタンスを起動、停止、削除、または再起動するには	222
NetScalerインスタンスファイルを削除する	223
NetScalerインスタンスファイルを削除するには	223

管理構成を適用する	223
NetScalerインスタンスに管理構成を適用するには	223
SSL証明書をインストールして管理する	223
証明書ファイルをSDXアプライアンスにアップロードする	224
SSL証明書ファイルをSDXアプライアンスにアップロードするには	224
SSL証明書ファイルをダウンロードしてバックアップを作成するには	224
SDXアプライアンスへのSSLキーファイルのアップロード	224
SDXアプライアンスにSSLキーファイルをアップロードするには	225
SSL キーファイルをダウンロードしてバックアップを作成するには	225
NetScaler インスタンスへの SSL 証明書のインストール	225
NetScaler インスタンスに SSL 証明書をインストールするには	225
NetScalerインスタンスでのSSL証明書の更新	226
NetScalerインスタンスでSSL証明書を更新するには	226
NetScalerインスタンス上のSSL証明書のポーリング	227
ポーリング間隔を構成するには	227
即時ポーリングを実行するには	227
NetScalerインスタンスでL2モードを許可する	228
インスタンスでL2モードを許可するには	229
インターフェースでの仮想MACの設定	229
SDX管理サービスでVMACを構成する	230
インターフェースまたはLAチャンネルにIPv4またはIPv6 VRIDを追加するには	231
SDXアプライアンスのNetScalerインスタンスで管理パーティションを設定するために、パーティションMACアドレスを生成する	231
VPX インスタンスの変更管理	233
VPX インスタンスの変更管理を表示するには	234
NetScaler インスタンスの構成の更新をポーリングするには	234
NetScalerインスタンスの監査テンプレートを構成するには	234
チャンネルメンバーインターフェースの自動リカバリ	235

NetScaler SDX™上でNetScalerインスタンスのディスク領域を拡張する	236
GUIを使用してNetScaler®インスタンスのディスク領域を拡張する	236
NetScalerインスタンスのディスク領域の割り当てと拡張	236
NetScalerインスタンスの監視	239
VPXインスタンスのプロパティを表示する	239
VPXインスタンスのプロパティを表示するには	239
NetScalerインスタンスの実行中および保存済み構成を表示する	241
NetScalerインスタンスの実行中および保存済み構成を表示するには	241
NetScaler インスタンスを Ping する	241
NetScaler インスタンスを Ping するには	241
NetScaler インスタンスのルートをトレースする	242
NetScaler インスタンスのルートをトレースするには	242
NetScaler インスタンスを再検出する	242
NetScalerインスタンスを再検出するには	242
ログを使用して操作とイベントを監視する	243
監査ログを表示する	243
タスクログの表示	244
タスクデバイスログの表示	244
タスクコマンドログの表示	244
イベントの表示	245
NetScaler SDXアプライアンスのユースケース	246
管理サービスとNetScalerインスタンスが同じネットワークにある場合の統合	246
この例に示すように NetScaler インスタンス 1 をプロビジョニングする	248
管理サービスとNetScalerインスタンスが異なるネットワークにある場合の統合	248
この例に示すようにNetScalerインスタンス1をプロビジョニングするには	250
セキュリティゾーン間の統合	250
各インスタンスに専用インターフェースを割り当てた統合	251
この例に示すように、NetScaler インスタンス 5 および 3 をプロビジョニングするには	253

複数のインスタンスによる物理ポート共有での統合	253
この例でNetScalerインスタンス7と4をプロビジョニングするには	255
NITRO API	256
NITROパッケージの取得	256
.NET SDK	257
システムAPI	257
設定API	258
リソースの作成	259
リソースの詳細を取得する	260
リソース統計を取得する	261
リソースを更新する	261
リソースを削除する	262
一括操作	263
例外処理	264
REST Web サービス	265
システム API	265
構成 API	269
リソースの作成	269
リソースの詳細と統計の取得	270
リソースを更新する	271
リソースを削除する	272
一括操作	272
例外処理	276
NITROの仕組み	276
ジャバ SDK	277
システムAPI	277
構成API	278
リソースの作成	278

リソースの詳細の取得	280
リソース統計の取得	280
リソースの更新	281
リソースの削除	282
一括操作	282
例外処理	284
fix	285

はじめに

NetScaler SDXアプライアンスは、複数のNetScaler仮想マシン（インスタンス）をプロビジョニングおよび管理できるマルチテナントプラットフォームです。SDXアプライアンスは、単一の管理者がアプライアンスを設定および管理し、ホストされている各インスタンスの管理をテナントに委任できるようにすることで、クラウドコンピューティングとマルチテナンシーの要件に対応します。SDXアプライアンスにより、アプライアンス管理者は各テナントに以下の利点を提供できます。

- 完全なインスタンスを1つ。各インスタンスには以下の特権があります。
 - 専用のCPUおよびメモリリソース
 - エンティティ用の個別のスペース
 - 選択したリリースとビルドを実行する独立性
 - ライフサイクルの独立性
- 完全に分離されたネットワーク。特定のインスタンス宛てのトラフィックは、そのインスタンスにのみ送信されます。

SDXアプライアンスは、アプライアンスに事前にプロビジョニングされているManagement Serviceを提供します。Management Serviceは、アプライアンス、Management Service、およびインスタンスを設定、管理、監視するためのユーザーインターフェイス（HTTPおよびHTTPSモード）とAPIを提供します。Citrix®自己署名証明書は、HTTPSサポートのために事前にパッケージ化されています。Citrixは、Management ServiceユーザーインターフェイスにアクセスするためにHTTPSモードを使用することを推奨します。

リリースノート

リリースノートには、特定のNetScalerソフトウェアのリリースまたはビルドにおける機能強化、変更、バグ修正、および既知の問題が記載されています。NetScaler SDXのリリースノートは、NetScalerリリースノートの一部として含まれています。

SDX 14.1の機能強化、既知の問題、およびバグ修正に関する詳細については、[NetScalerリリースノート](#)を参照してください。

Management Serviceユーザーインターフェイスの利用を開始する

アプライアンス、Management Service、および仮想インスタンスの構成、管理、監視を開始するには、ブラウザを使用してManagement Serviceユーザーインターフェイスに接続します。次に、アプライアンス上で仮想インスタンスをプロビジョニングします。

以下のサポートされているブラウザのいずれかを使用して、Management Serviceユーザーインターフェイスに接続できます。

- インターネット エクスプローラー
- グーグル クローム
- アップル サファリ
- モジラ ファイアフォックス

Management Serviceユーザーインターフェイスにログオンする

1. Webブラウザのアドレスフィールドに、次のいずれかを入力します。

`http://Management Service IP Address`

または

`https://Management Service IP Address`

2. ログインページで、**ユーザー名とパスワード**にManagement Serviceのユーザー名とパスワードを入力します。デフォルトのユーザー名は `nsroot` です。デフォルトのパスワードが機能しない場合は、アプライアンスのシリアル番号を入力してみてください。シリアル番号のバーコードはアプライアンスの背面にあります。初めてデフォルトの資格情報でログインした後、デフォルトの `nsroot` パスワードを変更する必要があります。管理者パスワードの変更については、「[デフォルトユーザーアカウントのパスワードの変更](#)」を参照してください。
3. 「オプションの表示」をクリックし、次の操作を行います。
 - a. **開始**リストで、ユーザーインターフェイスにログオンした直後に表示するページを選択します。利用可能なオプションは、ホーム、監視、構成、ドキュメント、ダウンロードで

す。たとえば、ログオン時にManagement Serviceに構成ページを表示させたい場合は、**開始リスト**で**構成**を選択します。

- b. **Timeout** に、セッションを期限切れにするまでの時間（分、時間、または日）を入力します。最小タイムアウト値は15分です。

Start in および **Timeout** の設定はセッション間で保持されます。これらのデフォルト値は、キャッシュをクリアした後にのみ復元されます。

4. **Login** をクリックして、Management Serviceユーザーインターフェイスにログオンします。

初期設定ウィザード

セットアップウィザードを使用すると、すべての初回設定を1つのフローで完了できます。

ウィザードを使用して、ネットワーク構成の詳細とシステム設定を構成したり、デフォルトの管理者パスワードを変更したり、ライセンスを管理および更新したりできます。

このウィザードを使用して、初期設定時にSDXアプライアンスに指定したネットワーク構成の詳細を変更することもできます。

ウィザードにアクセスするには、**Configuration > System** に移動し、**Set Up Appliance** の下にある **Setup Wizard** をクリックします。以下のパラメータの値を入力します。

- **Interface:** アプライアンスを管理ワークステーションまたはネットワークに接続する管理インターフェイス。可能な値: 0/1, 0/2。デフォルト: 0/1。
- **Gateway:** アプライアンスのサブネットからトラフィックを転送するルーターのIPアドレス。
- Management ServiceにIPv4アドレスを使用する場合は、IPv4チェックボックスを選択し、以下のパラメータの詳細を入力します。
 - **Appliance Management IP:** Webブラウザを使用してManagement Serviceにアクセスするために使用されるIPv4アドレス。
 - **Netmask:** SDXアプライアンスが配置されているサブネットマスク。
- **DNS:** プライマリDNSサーバーのIPv4アドレス。IPv6アドレスはプライマリDNSサーバーではサポートされていません。
- Management ServiceにIPv6アドレスを使用する場合は、IPv6チェックボックスを選択し、以下のパラメータの詳細を入力します。
 - **Management Service IP Address:** Webブラウザを使用してManagement Serviceにアクセスするために使用されるIPv6アドレス。

- **Gateway IPv6 Address:** アプライアンスのサブネットからトラフィックを転送するルーターのIPv4アドレス。
- プライマリDNSサーバーとは別に、追加のDNSサーバーとしてDNSサーバーのIPアドレスを追加するには、**Additional DNS**を選択します。IPアドレスはIPv4またはIPv6のいずれかです。

セットアップウィザードのネットワーク構成(/en-us/sdx/media/network-configuration-in-setup-wizard.png)

重要！

セキュリティを向上させるため、Citrix®はアプライアンスのサポート機能を無効にしておくことを推奨します。アプライアンスのサポート機能を無効にするには、**System > Network Configuration**に移動し、**Configure Appliance supportability**チェックボックスをオフにします。

System Settingsで、Management ServiceとNetScalerインスタンスがセキュアなチャンネルを介してのみ通信するように指定できます。Management Serviceユーザーインターフェイスへのアクセスを制限することもできます。クライアントはhttpsを使用してのみManagement Serviceユーザーインターフェイスにログオンできます。

Management ServiceとCitrix Hypervisorのタイムゾーンを変更できます。デフォルトのタイムゾーンはUTCです。**Change Password**チェックボックスを選択し、新しいパスワードを入力することで、管理者パスワードを変更できます。

ライセンスの管理では、ライセンスを管理および割り当てることができます。ハードウェアシリアル番号 (HSN) またはライセンスアクセスコードを使用してライセンスを割り当てることができます。または、ライセンスがすでにローカルコンピューターに存在する場合は、アプライアンスにアップロードできます。

アプライアンスでライセンスを選択し、**Done**をクリックして初期設定を完了します。

SDXアプライアンスでインスタンスをプロビジョニングする

Management Serviceを使用して、SDXアプライアンスに1つ以上のNetScalerまたはサードパーティインスタンスをプロビジョニングできます。インストールできるインスタンスの数は、購入したライセンスによって異なります。追加されたインスタンスの数がライセンスで指定された数と等しい場合、Management Serviceはそれ以上のインスタンスのプロビジョニングを許可しません。

サードパーティインスタンスのプロビジョニングについては、[Third-Party Virtual Machines](#)を参照してください。

コンソールアクセス

Management Serviceインターフェイスから、NetScalerインスタンス、Management Service、Citrix Hypervisor、およびサードパーティVMのコンソールにアクセスできます。このアクセスは、SDXアプライアンスでホストされているインスタンスのデバッグとトラブルシューティングに役立ちます。

VMのコンソールにアクセスするには、インスタンスリストに移動し、リストからVMを選択し、アクションリストでコンソールアクセスをクリックします。

Management ServiceまたはCitrix Hypervisorのコンソールにアクセスするには、**構成 > システム**に移動し、**コンソールアクセス**の下にある**Management Service**または**Citrix Hypervisor**リンクをクリックします。

注: Internet Explorerブラウザはコンソールアクセスをサポートしていません。Citrixは、Management Service HTTPSセッションを介してのみコンソールアクセス機能を使用することを推奨します。

Management Serviceの統計

ダッシュボードには、SDXアプライアンス上のManagement Serviceによるメモリ、CPU、ディスクリソースの使用状況を監視するためのManagement Service統計が含まれるようになりました。



Management ServiceおよびNetScalerインスタンスへのシングルサインオン

ユーザー資格情報を使用してManagement Serviceにログオンした後、インスタンスにログオンするためにユーザー資格情報を再度入力する必要はありません。デフォルトでは、**タイムアウト値**は30分に設定されており、構成タブは新しいブラウザウィンドウで開かれます。

ホームページの管理

Management Serviceのホームページでは、SDXアプライアンスのパフォーマンスとアプライアンスにプロビジョニングされたインスタンスの概要を確認できます。SDXアプライアンスとインスタンスに関する情報は、要件に応じて追加および削除できるガジェットに表示されます。

以下のガジェットは、デフォルトでホームページで利用できます。

- **システムリソース:** アプライアンス上のCPUコアの総数、SSLチップの総数、空きSSLチップの数、合計メモリ、および空きメモリを表示します。
- **システムCPU | メモリ使用率 (%):** アプライアンスのCPUとメモリの使用率をグラフィカル形式で表示します。
- **システムWAN/LANスループット (Mbps):** SDXアプライアンスの受信および送信トラフィックの合計スループットを、リアルタイムでプロットされ、定期的に更新されるグラフで表示します。
- **NetScalerインスタンス:** NetScalerインスタンスのプロパティを表示します。表示されるプロパティは、名前、VMステータス、インスタンスステータス、IPアドレス、Rx (Mbps)、Tx (Mbps)、HTTP要求/秒、CPU使用率 (%), およびメモリ使用率 (%) です。注: 初回ログオン時には、アプライアンスにインスタンスがプロビジョニングされていないため、ホームページにはNetScalerインスタンスに関連するデータは表示されません。
- **ヘルス監視イベント:** 最後の25件のイベントを、重大度、メッセージ、およびイベント発生日時とともに表示します。

ホームページでは、次のことができます。

- NetScalerインスタンスの詳細の表示と非表示

「名前」列でインスタンスの名前をクリックすると、特定のNetScalerインスタンスの詳細を表示および非表示にできます。また、「すべて展開」をクリックしてすべてのインスタンスノードを展開したり、「すべて折りたたむ」をクリックしてすべてのインスタンスノードを折りたたんだりすることもできます。

- ガジェットの追加と削除

他のシステム情報を表示するためにガジェットを追加することもできます。

これらのガジェットを追加するには、ホームページの右上隅にある矢印 (<<) ボタンをクリックし、検索ボックスにキーワードを入力して、Go をクリックします。使用できる文字は、a-z、A-Z、0-9、\、\$、*、_ です。検索ボックスに文字を入力せずに Go をクリックすると、利用可能なすべてのガジェットが表示されます。ガジェットが表示されたら、Add to dashboard をクリックします。

現在、ホームページには次のガジェットを追加できます。

- **ハイパーバイザーの詳細:** ハイパーバイザーの詳細ガジェットには、Citrix Hypervisorの稼働時間、エディション、バージョン、iSCSI修飾名 (IQN)、製品コード、シリアル番号、ビルド日、およびビルド番号に関する詳細が表示されます。

- 。 **ライセンス:** ライセンスガジェットには、SDXハードウェアプラットフォーム、プラットフォームでサポートされるインスタンスの最大数、サポートされる最大スループット (Mbps)、および利用可能なスループット (Mbps) の詳細が表示されます。

デフォルトでホームページで利用可能なガジェットを削除した場合、そのガジェットを検索してホームページに再度追加できます。

ポート

SDXアプライアンスが正常に機能するためには、次のポートが開いている必要があります。

種類	ポート	詳細
TCP	80	着信HTTP（GUIおよびNITRO）リクエストに使用されます。SDX管理サービスインターフェースにアクセスするための主要なインターフェースの1つです。
TCP	443	着信セキュアHTTP（GUIおよびNITRO）リクエストに使用されます。SDX管理サービスインターフェースにアクセスするための主要なインターフェースの1つです。
TCP	22	SDX管理サービスインターフェースへのSSHおよびSCPアクセスに使用されます。
UDP	162	SDX管理サービスインターフェースは、SDXアプライアンスでホストされているNetScalerインスタンスからのSNMPトラップをリッスンします。
UDP	161	SDX Management Service インターフェースは、SNMPウォーク/get リクエストをリッスンします。

データガバナンス

Console Advisory Connectとは何ですか？

Console Advisory Connectは、NetScaler SDXアプライアンスをNetScaler Consoleサービスにシームレスにオンボーディングするための機能です。この機能により、NetScaler SDXアプライアンスはNetScaler Consoleサービスに自動的かつ安全に接続し、システム、使用状況、テレメトリデータを送信できます。このデータに基づいて、NetScaler ConsoleサービスでNetScalerインフラストラクチャに関するインサイトと推奨事項が得られます。

Console Advisory Connect機能を使用し、NetScaler SDXアプライアンスをNetScaler Consoleサービスにオンボーディングすることで、オンプレミスかクラウドかにかかわらず、すべてのNetScalerおよびNetScaler Gatewayアセットを管理できます。さらに、パフォーマンスの問題、高いリソース使用率、重大なエラーなどを迅速に特定するのに役立つ豊富な可視化機能にアクセスできるというメリットがあります。NetScaler Consoleサービスは、NetScalerインスタンスとアプリケーションに幅広い機能を提供します。NetScaler Consoleサービスの詳細については、[NetScaler Console Service](#)を参照してください。

重要

- このドキュメントはNetScaler SDXアプライアンスに関するものです。NetScalerアプライアンスの詳細については、[NetScalerアプライアンス向けConsole Advisory Connectの概要](#)を参照してください。
- NetScaler GatewayもConsole Advisory Connect機能をサポートしています。便宜上、NetScaler Gatewayアプライアンスは以降のセクションでは明示的に言及されていません。

注: Console Advisory Connect機能はNetScalerインスタンスおよびNetScaler Gatewayインスタンス向けにリリースされています。ただし、NetScaler Consoleサービス上の対応する機能は今後のリリースで利用可能になります。この機能の価値は、NetScaler Consoleサービスのリリースとともに間もなく発揮されるでしょう。Citrixは、それが実現した際にこの注記を更新します。この新機能のメリットは、NetScaler Consoleサービスでリリースされた後に利用できます。

NetScaler Consoleサービスとは何ですか？

NetScaler Consoleサービスは、NetScaler SDXインスタンスに関する分析情報と、アプリケーションの健全性、パフォーマンス、セキュリティに関するキュレーションされた機械学習ベースの推奨事項を提供することで、NetScaler SDXインスタンスの管理、監視、オーケストレーション、自動化、トラブルシューティングを支援するクラウドベースのソリューションです。詳細については、[NetScaler Console service Overview](#)を参照してください。

Console Advisory Connectの有効化方法？

NetScaler SDXをリリース13.1にインストールまたはアップグレードすると、Console Advisory Connectはデフォルトで有効になります。

Console Advisory Connectで取得されるデータ？

Console Advisory Connectを使用して、以下の詳細が取得されます。

- **NetScaler SDXの詳細**

- 管理IPアドレス
- プラットフォームの説明
- プラットフォームの種類
- ホスト名
- システムID
- エンコードされたシリアルID
- バージョン
- シリアルID
- ホストID
- タイプ
- ビルドタイプ

- **主な使用状況メトリック**

- 管理CPU使用率
- メモリ使用率
- CPU使用率
- システム稼働時間

- 。 システム日時

データの使用方法？

データを収集することで、NetScalerはNetScaler SDXのインストールに関するタイムリーで詳細な洞察を提供できます。これには以下が含まれます。

- **主要メトリック。** CPU、メモリ、スループット、SSLスループットに関する主要メトリックの詳細、およびNetScaler SDXインスタンス上の異常な動作の強調表示。
- **重大なエラー。** NetScalerインスタンスで発生した可能性のある重大なエラー。
- **展開アドバイザリ。** スタンドアロンモードで展開されているが、スループットが高く、単一障害点に対して脆弱なNetScalerインスタンスを特定します。

収集されたデータの保持期間？

収集されたデータはすべて、13か月を超えて保持されることはありません。

NetScalerからConsole Advisory Connect機能を無効にしてサービスの使用を終了することを決定した場合、以前に収集されたデータはすべて30日後に削除されます。

データはどこに保存され、どの程度安全ですか？

Console Advisory Connectによって収集されたすべてのデータは、米国、欧州連合、オーストラリアおよびニュージーランド（ANZ）の3つの地域のいずれかに保存されます。詳細については、「[地理的考慮事項](#)」を参照してください。

データは、データベース層で厳格なテナント分離により安全に保存されます。

Console Advisory Connectを無効にする方法？

Console Advisory Connectを介したデータ収集を無効にする場合は、「[Console Advisory Connectを有効/無効にする方法](#)」を参照してください。

NetScaler SDXアプライアンス向け Console Advisory Connectの概要

NetScaler Consoleサービスは、NetScaler SDXアプライアンスの管理、監視、オーケストレーション、自動化、トラブルシューティングを支援するクラウドベースのソリューションです。また、アプリケーションの健全性、パフォーマンス、セキュリティに関する分析情報と、厳選された機械学習ベースの推奨事項も提供します。詳細については、[NetScaler Consoleサービス](#)を参照してください。

Console Advisory Connectは、NetScaler SDXアプライアンスをNetScaler Consoleサービスにシームレスにオンボーディングするための機能です。この機能により、NetScaler SDXアプライアンスとNetScaler Consoleサービスが統合ソリューションとして機能し、お客様に多大なメリットを提供します。

Console Advisory Connect機能により、NetScaler SDXインスタンスはNetScaler Consoleサービスに自動的に接続し、システム、使用状況、テレメトリデータを送信します。このデータを使用して、NetScaler Consoleサービスは、パフォーマンス問題の迅速な特定や高いリソース使用率など、NetScaler SDXインフラストラクチャに関する洞察と推奨事項を提供します。

NetScaler Consoleサービスの機能を活用するには、NetScaler SDXアプライアンスをNetScaler Consoleサービスにオンボーディングすることを選択できます。オンボーディングプロセスではConsole Advisory Connectを使用し、お客様にとってシームレスで迅速なエクスペリエンスを実現します。

注意点

- Console Advisory Connectは、NetScaler MPX、SDX、VPXインスタンス、およびNetScaler Gatewayアプライアンスで利用可能になりました。

詳細については、[データガバナンス](#)を参照してください。

Console Advisory ConnectはNetScaler Consoleサービスをどのようにサポートするか？

NetScalerのConsole Advisory Connect機能がNetScaler Consoleサービスとどのように連携するかの概要ワークフローを以下に示します。

1. NetScaler SDXアプライアンスのConsole Advisory Connect機能は、定期的なプローブ要求を使用してNetScaler Consoleサービスに自動接続します。
2. この要求にはシステム、使用状況、テレメトリデータが含まれており、これを使用してNetScaler Consoleサービスは、パフォーマンス問題の迅速な特定や高いリソース使用率など、NetScalerインフラストラクチャに関する洞察と推奨事項を提供します。
3. 洞察と推奨事項を確認し、NetScaler SDXアプライアンスをNetScaler Consoleサービスにオンボーディングして、NetScaler SDXアプライアンスの管理を開始できます。
4. オンボーディングを決定すると、Console Advisory Connect機能がオンボーディングをシームレスに完了するのに役立ちます。

Console Advisory ConnectがサポートするNetScalerのバージョン？

Console Advisory Connectは、すべてのNetScalerプラットフォームおよびすべてのアプライアンスモデル (MPX、VPX、SDX) でサポートされています。NetScalerリリース13.0ビルド64.xx以降、Console Advisory ConnectはNetScaler SDXアプライアンスでデフォルトで有効になっています。

Console Advisory Connectを有効にする方法？

既存のNetScalerのお客様で、NetScalerリリース13.0ビルド64.xxにアップグレードする場合、Console Advisory Connectはアップグレードプロセスの一部としてデフォルトで有効になります。

新規のNetScalerのお客様で、NetScalerリリース13.0ビルド64.xxをインストールする場合、Console Advisory Connectはインストールプロセスの一部としてデフォルトで有効になります。

注

新しいNetScalerアプライアンスとは異なり、既存のNetScaler SDXアプライアンスはCitrix Insight Service (CIS) またはCall Homeを介して経路を見つけます。

Console Advisory Connectを有効化および無効化する方法？

Console Advisory Connectは、CLI、GUI、またはNITRO APIメソッドから有効化および無効化できます。

CLIの使用

CLIを使用してConsole Advisory Connectを有効にするには

コマンドプロンプトで、次のように入力します。

```
set autoreg_setting autoreg=true
```

CLIを使用してConsole Advisory Connectを無効にするには

コマンドプロンプトで、次のように入力します。

```
set autoreg_setting autoreg=false
```

CLIを使用してConsole Advisory Connectの設定を表示するには

```
show autoreg_setting

autoreg: true

is_banner_displayed: true

Done
```

GUIの使用

NetScaler GUI を使用して Console Advisory Connect を無効にするには

1. **System** に移動します。**System** ページで、**System Settings** セクションの **Configure Console Advisory Connect** をクリックします。
2. **Configure NetScaler Console Parameters** ページで、**Enable Console Advisory Connect** のチェックを外し、**OK** をクリックします。



NITRO API の使用

NITRO コマンドを使用して Console Advisory Connect を無効にできます。

```
curl -X PUT -H "Content-Type:application/json" http://192.0.2.10/nitro/v1/config/sdx_autoreg -d '{"sdx_autoreg":{"autoreg":"false"}}' -u nsroot:Test@1
```

NetScaler Console 組み込みエージェントの動作

NetScaler リリース 13.0 ビルド 61.xx 以降、NetScaler SDX インスタンスには、Console Advisory Connect 機能を持つ組み込みエージェントが搭載されています。NetScaler SDX インスタンスで利用可能な NetScaler Console 組み込みエージェントは、アクティブなデーモンのように起動し、NetScaler Console サービスと通信します。NetScaler Console サービスとの通信が確立されると、組み込みエージェントは定期的に最新のソフトウェアバージョンに自動アップグレードされます。

参照

Console Advisory Connect の詳細については、次のトピックを参照してください。

- データガバナンス: [データガバナンス](#)。
- NetScaler Console サービス: [NetScaler Console サービス](#)。

シングルバンドルアップグレード

シングルバンドルアップグレードを使用すると、シングルバンドルイメージ (SBI) と呼ばれる単一のイメージファイルを使用して、NetScaler VPXインスタンスイメージを除くすべてのNetScaler SDXアプライアンスコンポーネントをアップグレードできます。このイメージを使用すると、すべてのコンポーネントを1つのステップでアップグレードでき、さまざまなコンポーネント間の非互換性の可能性を排除できます。シングルバンドルアップグレードは、アプライアンスが常にCitrixがテストしサポートしているバージョンで実行されていることを保証します。すべてのSDXコンポーネントが1つのファイルに結合されているため、SDXイメージファイルはManagement Serviceイメージファイルよりも大きくなります。

イメージのファイル名は `build-sdx-14.1-<build_number>.tgz` の形式です。Management ServiceがSDX 14.1にアップグレードされた後、新しいGUIにはCitrix Hypervisorイメージファイル、補足パック、またはホットフィックスをアップロードするオプションが表示されません。これらのオプションがないのは、SDX 14.1が個々のコンポーネントのアップグレードをサポートしていないためです。

このドキュメントでは、アップグレード前の主要な考慮事項とアプライアンスをアップグレードする手順について説明します。

NetScaler SDXのアップグレード前の重要な考慮事項

このセクションでは、NetScaler SDXアプライアンスをアップグレードする前に確認する必要がある重要な考慮事項について説明し、スムーズで成功するアップグレードプロセスを保証します。

必須のバックアップ

アップグレードを開始する前に、完全なシステムバックアップを実行してください。このバックアップは、SDXアプライアンスの外部の安全な場所に保管してください。複数ステップのアップグレードを実行する場合は、各段階の前に新しいバックアップを作成してください。

推定メンテナンス期間

アップグレード、クリーンインストール、または工場出荷時設定へのリセットにかかる時間は、現在のソフトウェアバージョンとターゲットリリースバージョンによって異なります。

- **標準アップグレード:** 通常、1～2時間かかります。

- **複雑なアップグレード:** XenServerのバージョン変更（例：バージョン6.5、7、8間の移行）やハードウェアレベルの更新（NIC/LOM）を伴う移行には、大幅に長い時間が必要です。
- **延長される期間:** 以前のビルド（13.1または14.1-29.x以前）からバージョン14.1-66.x（またはそれ以降）へのアップグレードには、5～6時間かかる場合があります。この延長された時間は、XenServer 8、Fortvilleファームウェア、Mellanoxドライバー、およびSVMデータベースのバンドルされた更新によるものです。

注記:

アップグレードプロセスが開始されたら、中断しないでください。プロセスを中断すると、システムの不安定性やデータ損失につながる可能性があります。

段階的なアップグレードパス

アップグレードプロセスを最適化するには、14.1-66.x以降にアップグレードする際に、単一のジャンプではなく段階的なアップグレードパスを使用してください。

推奨されるアップグレードパス:

この推奨パスに従ってください。

以前のビルド → 14.1-47.x → 14.1-66.x (またはそれ以降)

注:

- NetScaler SDXアプライアンスをリリース13.1以降にインストールまたはアップグレードすると、Console Advisory Connectはデフォルトで有効になります。詳細については、[データガバナンス](#)および[Console Advisory Connect](#)を参照してください。
- Lights Out Management (LOM) ファームウェアはSBIに追加されており、Citrix®のお客様はLOMを個別にアップグレードする必要はありません。LOMの更新には、アップグレードプロセスに最大30分かかる場合があります。LOMの詳細については、[NetScaler SDX アプライアンスのLights out managementポート](#)を参照してください。

SDX 9100および16000プラットフォームの場合、新しいLOMファームウェアを含むSBIにアップグレードした後、LOMの更新を手動でトリガーする必要があります。

前提条件

1. アップグレードを開始する前に、SDXをバックアップしてください。
2. NITROまたはNetScaler® Console (ADM) を介してアップグレードする前に、サポートされているSDXプラットフォームリストを確認してください。

注意点

- Citrix Hypervisorのバージョンが6.1以前の場合、14.1へのアップグレードはサポートされていません。
- シングルバンドルアップグレードは、最大90分かかる多段階プロセスです。
- まず、Management Service が新しいバージョンにアップグレードされます。アップグレード中に、Management Service への接続が失われる可能性があります。アップグレードのステータスを監視するために、Management Service に再接続してください。
- 次に、Management Service は Citrix Hypervisor™ をアップグレードし、アプライアンスの残りのアップグレードを完了します。
- Citrix Hypervisor のアップグレード中にアプライアンスを再起動しないでください。
- Citrix は、Citrix Hypervisor のアップグレードを監視するために、Citrix Hypervisor シリアルコンソール（または LOM コンソール）を使用することを推奨します。
- アップグレードプロセスを中断しないことをお勧めします。シリアルコンソールで進行状況を監視できます。また、このプロセス中に再起動や電源の問題が発生しないことを確認してください。

アプライアンス全体を 14.1 にアップグレードする

注: アップグレードプロセスでは、すべての VPX インスタンスを含む SDX アプライアンス全体が複数回再起動されます。この手順を実行する前に、VPX インスタンスが HA セットアップにある場合は、すべてのプライマリ HA ノードをセカンダリノードにフェイルオーバーしてください。HA 展開がない場合は、それに応じてダウンタイムを計画してください。

アプライアンスをアップグレードするには:

1. Single Bundle Image (SBI) ファイルをアップロードし、**Configuration > Management Service > Software Images** に移動して、**Upload** をクリックします。
2. **設定 > システム > システム管理** に移動します。
3. System Administration グループで、**Upgrade Appliance** をクリックします。アップグレードプロセスには数分かかります。

アップグレード前に、Management Service は次の情報を表示します。

- SBI ファイル名。
- アプライアンスで実行されている SDX の現在のバージョン。
- アプライアンスがアップグレードされる選択されたバージョン。
- アプライアンスのアップグレードにかかるおおよその時間。
- その他の情報。

Upgrade Appliance をクリックする前に、画面に表示されているすべての情報を確認してください。アップグレードプロセスは一度開始すると中止できません。

サポートされているアップグレードパス

ファクトリーイメージ	12.1へのアップグレード	13.1へのアップグレード	14.1へのアップグレード
10.5 (EoL)	サポートされていません。FRUブートドライブを新しいイメージに交換してください。	サポートされていません。FRUブートドライブを新しいイメージに交換してください。	サポートされていません。FRUブートドライブを新しいイメージに交換してください。
11.0 (EoL)	サポートされていません。FRUブートドライブを新しいイメージに交換してください。	サポートされていません。FRUブートドライブを新しいイメージに交換してください。	サポートされていません。FRUブートドライブを新しいイメージに交換してください。
11.1 (EoL)	サポートされています (12.1-56.x 以降まで)	バージョン12.1までのみサポート	バージョン13.1までのみサポート
12.1	推奨されません	サポートされています	バージョン13.1までのみサポート
13.0 (EoL)	サポートされていません。13.0からのアップグレードは避けてください。	サポートされていません。13.0からのアップグレードは避けてください。	サポートされていません。13.0からのアップグレードは避けてください。
13.1	N/A	サポート対象	サポート対象

ファクトリーイメージ	12.1へのアップグレード	13.1へのアップグレード	14.1へのアップグレード
14.1	N/A	N/A	サポート対象

関連情報

[NetScaler SDX ハードウェア-ソフトウェア互換性マトリックス](#)

SDX XenServer® 8 へのアップグレード

SDX SBI の XenServer 7.1.2 は、リリース 14.1-34.x 以降で XenServer 8 にアップグレードされます。

SBI 14.1-47.x 以降でサポートされるNetScalerプラットフォーム

- SDX 8900

SBI 14.1-34.x 以降でサポートされるNetScalerプラットフォーム

- SDX 9100
- SDX 16000
- SDX 15000-50G
- SDX 15000-25G
- SDX 26000-50S
- SDX 26000
- SDX 26000-100G
- SDX 25000
- SDX 25000A

SBI 14.1-34.x以降でサポートされていないNetScalerプラットフォーム

注:

- SDX 14000 FIPSはサポートされていません。
- EOLに達したプラットフォームはサポートされていません。
- SDX 8900はSBI 14.1-34.xではサポートされていませんが、SBI 14.1-47.x以降ではサポートされています。

- SDX 8xxx
- SDX 11500、SDX 13500、SDX 14500、SDX 16500、SDX 18500、SDX 20500
- SDX 115xx
- SDX 22xxx および SDX 24xxx

アップグレードマトリックス

XenServer 7 (バージョン 13.0 以降) を搭載した SBI は、XenServer 8 を搭載した SBI にのみアップグレードできます。XenServer 6.5 (バージョン 12.1) 以前を搭載した SBI から XenServer 8 を搭載した SBI への直接アップグレードはサポートされていません。

実行中の SBI バージョン	ターゲット SBI バージョン	アップグレードパス
12.1 (XenServer 6.5) またはそれ以前	14.1 (XenServer 8)	13.1 (XenServer 7) にアップグレードしてから、14.1-34.x (XenServer 8) 以降にアップグレード
13.0 (XenServer 7.1)	14.1 (XenServer 8)	サポートされています
13.1 (XenServer 7.1)	14.1 (XenServer 8)	サポートされています

ハードウェアプラットフォーム	13.1	14.1
SDX 14000 FIPS	シングルバンドルアップグレードの13.1リリーストレインは、2027年9月までサポートされます。	14.1-29.x はシングルバンドルアップグレードでサポートされており、2028年3月1日までサポートが継続されます。

ダウングレードマトリックス

工場出荷時のSBIバージョン	実行中のSBIバージョン	ターゲットSBIバージョン	クリーンインストールパス
12.1 (XenServer 6.5)	14.1 (XenServer 8)	12.1 (XenServer 6.5)	サポートされていません
12.1 (XenServer 6.5)	14.1 (XenServer 8)	任意 (XenServer 7.1以降)	サポート対象
12.1 (XenServer 6.5)	14.1 または 13.1 (XenServer 7.1)	14.1 (XenServer 8)	サポート対象外
12.1 (XenServer 6.5)	12.1 (XenServer 6.5)	14.1 (XenServer 8)	サポート対象外
13.1 (XenServer 7.1)	14.1 (XenServer 8)	任意 (XenServer 7.1以降)	サポート対象
13.1 (XenServer 7.1)	14.1 または 13.1 (XenServer 7.1)	14.1 (XenServer 8)	実行中のバージョンが14.1-17+および13.1-53+の場合のみサポートされます
XenServer 6.5以前の任意のSBI	任意	14.1 (XenServer 8)	サポート対象外

サポートされているVPXバージョン

SDXがサポートされていないVPXバージョンを実行している場合、アップグレードはブロックされます。このような場合、プラットフォームをXenServer 8にアップグレードする前に、すべてのVPXバージョンをサポートされているバージョンにアップグレードする必要があります。

VPXバージョン	コメント
14.1	サポート対象
13.1	サポート対象
13.0以前	サポート対象外

制限事項

1. SBIバージョン14.1-34.xは、SDX 14000、SDX 14000 FIPS、SDX 8900ではサポートされていません。SDX 8900のサポートは、SBIバージョン14.1-47.x以降で利用できます。SDX 8900、SDX 14000、SDX 14000 FIPSでは、VPXバージョンを14.1-34.x以降にアップグレードできません。
2. 次のいずれかの条件が満たされている場合、SDXバージョン14.1-34.x以降へのアップグレードはサポートされません。
 - お使いのプラットフォームはサポートされていません。ただし、VPXバージョンを14.1-34.x以降にアップグレードすることはできます。
 - SDXがSBI 12.1以前を実行している。
 - SDXがXenServer 6.5以前を使用している。
 - SDX上のVPXインスタンスがサポートされていないバージョンを実行している。
 - SDXのローカルストレージの空き容量が34 GB未満である（SDX 9100およびSDX 16000を除く）。
3. 次のいずれかの条件が満たされている場合、リリース14.1-34.x以降へのクリーンインストールはサポートされません。
 - SDXがSBI 12.1以前を実行している。
 - SDXがXenServer 6.5以前を使用している。
 - SDX工場出荷バージョンは12.1以前です。
4. SDXが14.1-34.x以降で実行されている場合、バージョン12.1以前へのクリーンインストールはサポートされていません。

NetScalerインスタンスのアップグレード

注

- NetScaler SDXアプライアンスをリリース13.1にインストールまたはアップグレードすると、Console Advisory Connectがデフォルトで有効になります。詳細については、[データガバナンス](#)および[Console Advisory Connect](#)を参照してください。

NetScalerインスタンスのアップグレードプロセスには、ビルドファイルのアップロードと、その後のNetScalerインスタンスのアップグレードが含まれます。

重要

Management Serviceを使用したADCインスタンスのダウングレードはサポートされていません。ダウングレードするには、インスタンスCLIを使用してください。

NetScalerインスタンスをアップグレードする前に、NetScalerソフトウェアイメージをNetScaler SDXアプライアンスにアップロードしてください。新しいインスタンスをインストールするには、NetScaler XVAファイルが必要です。

ソフトウェアイメージペインで、次の詳細を表示できます。

- **名前:** NetScalerインスタンスソフトウェアイメージファイルの名前。ファイル名にはリリース番号とビルド番号が含まれます。たとえば、ファイル名 `build-13.1-49.13_nc_64.tgz` はリリース13.1ビルド49.13を指します。
- **最終更新日時:** ファイルが最後に変更された日付。
- **サイズ:** ファイルのサイズ（MB単位）。

ソフトウェアイメージをアップロードするには

1. ナビゲーションペインで、NetScalerを展開し、ソフトウェアイメージをクリックします。
2. ソフトウェアイメージペインで、**アップロード**をクリックします。
3. NetScalerソフトウェアイメージのアップロードダイアログボックスで、**参照**をクリックし、アップロードするNetScalerイメージファイルを選択します。
4. 「**アップロード**」をクリックします。イメージファイルがNetScaler Software Imagesペインに表示されます。

ビルドファイルをダウンロードしてバックアップを作成するには

1. Software Imagesペインで、ダウンロードするファイルを選択し、「**ダウンロード**」をクリックします。
2. メッセージボックスで、「**保存**」リストから「**名前を付けて保存**」を選択します。
3. 「名前を付けて保存」メッセージボックスで、ファイルを保存する場所を参照し、「**保存**」をクリックします。

XVAファイルをアップロードするには

1. ナビゲーションペインでNetScalerを展開し、「**Software Images**」をクリックします。
2. Software Imagesペインで、「**XVA Files**」タブの「**アップロード**」をクリックします。

3. 「**NetScaler XVAファイルのアップロード**」ダイアログボックスで、「**参照**」をクリックし、アップロードするNetScaler XVAファイルを選択します。
4. 「**アップロード**」をクリックします。XVAファイルが「**XVA Files**」ペインに表示されます。

XVAファイルをダウンロードしてバックアップを作成するには

1. XVA Filesペインで、ダウンロードするファイルを選択し、「**ダウンロード**」をクリックします。
2. メッセージボックスで、保存リストから「**名前を付けて保存**」を選択します。
3. 「**名前を付けて保存**」メッセージボックスで、ファイルを保存する場所を参照し、「**保存**」をクリックします。

NetScaler VPXインスタンスのアップグレード

Management Serviceを使用して、アプライアンスで実行されている1つ以上のVPXインスタンスをアップグレードできます。インスタンスをアップグレードする前に、正しいビルドをSDXアプライアンスにアップロードしていることを確認してください。

NetScaler Consoleサービスを使用してVPXインスタンスをアップグレードすることもできます。

インスタンスのアップグレードを開始する前に、ライセンスフレームワークとライセンスの種類を理解していることを確認してください。ソフトウェアエディションのアップグレード（標準エディションからエンタープライズエディションへ、またはエンタープライズエディションからプラチナエディションへなど）には、新しいライセンスが必要になる場合があります。また、以下にも注意してください。

- 設定の損失を防ぐため、インスタンスをアップグレードする前に、各インスタンスの設定を保存してください。
- インスタンスノードから個々のインスタンスをアップグレードすることもできます。これを行うには、インスタンスノードからインスタンスを選択します。詳細ペインでインスタンスを選択し、ドロップダウンメニューでをクリックします。

重要

- SDX Management Serviceを使用し、VPX GUIを使用せずにVPXインスタンスをアップグレードする場合、アップグレードイメージはバックアップファイルの一部となり、インスタンスをスムーズに復元できます。
- 設定にクラシックポリシーが含まれている場合、インスタンスのアップグレード中に「サポートされていないクラシックポリシーが見つかりました」というエラーが表示されることがあります。そのような場合は、クラシックポリシーをアドバンストポリシーに手動で変換する必要があります。詳細については、[Netscaler Notice of Status Change Announcement for Classic Policy Based Features and Functionalities](#)を参照してください。

以下はエラーメッセージの例です。

**VPXインスタンスをアップグレードするには**

1. **構成**タブのナビゲーションペインで、**NetScaler**をクリックします。
2. 詳細ペインの**NetScaler構成**で、**アップグレード**をクリックします。
3. **NetScalerのアップグレード**ダイアログボックスのソフトウェアイメージで、アップグレードしたいバージョンのNetScalerアップグレードビルドファイルを選択します。
4. **インスタンスIPアドレス**ドロップダウンリストから、アップグレードしたいインスタンスのIPアドレスを選択します。
5. **OK**をクリックし、次に**閉じる**をクリックします。

関連情報

NetScaler SDX ハードウェア-ソフトウェア互換性マトリックス([/ja-jp/citrix-hardware-platforms/sdx/supported-versions.html](#))

SDXアプライアンスの管理と監視

NetScaler SDXアプライアンスが稼働を開始した後、Management Serviceユーザーインターフェイスからアプライアンスを管理および監視するためのさまざまなタスクを実行できます。

SDXアプライアンスのネットワーク構成を変更する

初期設定時にSDXアプライアンスに提供したネットワーク構成の詳細を変更できます。

SDXアプライアンスのネットワーク構成を変更するには、**System**をクリックします。**System**ページの**Setup Appliance**グループで、**Network Configuration**をクリックし、ウィザードに詳細を入力します。

注:

Network Configurationで、Citrix Hypervisor™へのアクセスを有効にすると、「アクセスは6時間後に自動的に無効になります」という警告メッセージが表示されます。

デフォルトユーザーアカウントのパスワードを変更する

デフォルトのユーザーアカウントは、NetScaler SDXアプライアンスのすべての機能への完全なアクセスを提供します。セキュリティを維持するため、デフォルトの管理者アカウントは必要な場合にのみ使用してください。職務上、完全なアクセスが必要な個人だけが、デフォルトの管理者アカウントのパスワードを知っている必要があります。Citrixは、デフォルトの管理者パスワードを頻繁に変更することを推奨しています。パスワードを紛失した場合は、アプライアンス設定を工場出荷時のデフォルトに戻すことでパスワードをデフォルトにリセットし、その後パスワードを変更できます。

デフォルトユーザーアカウントのパスワードを変更するには、**System > User Administration > Users**をクリックします。ユーザーを選択し、**Edit**をクリックしてパスワードを変更します。

アプライアンスのタイムゾーンを変更する

Management ServiceとCitrix Hypervisorのタイムゾーンを変更できます。デフォルトのタイムゾーンはUTCです。

タイムゾーンを変更するには、**System**をクリックし、**System Settings**グループで**Change Time Zone**をクリックします。

アプライアンスのホスト名を変更する

System > System Settings > Change Hostnameに移動して、Management Serviceのホスト名を変更できます。Citrix Hypervisorのホスト名は、バックアップ/復元操作中にバックアップおよび復元されます。構成のリセット中、Citrix Hypervisorのホスト名はデフォルト値「netscaler-sdx」にリセットされます。

VLANフィルタリング

VLANフィルタリングは、物理ポートを共有するVPXインスタンス間のデータ分離を提供します。たとえば、2つの異なるVLAN上に2つのVPXインスタンスを設定し、VLANフィルタリングを有効にすると、一方のインスタンスはもう一方のインスタンスのトラフィックを表示できません。

VLANフィルタリングが無効になっている場合、すべてのインスタンスはタグ付きまたはタグなしのブロードキャストパケットを見ることができますが、パケットはソフトウェアレベルで破棄されます。VLANフィルタリングが有効になっている場合、各タグ付きブロードキャストパケットは、対応するタグ付きVLANに属するインスタンスにのみ到達します。どのインスタンスも対応するタグ付きVLANに属していない場合、パケットはハードウェアレベル（NIC）で破棄されます。

インターフェイスでVLANフィルタリングが有効になっている場合、そのインターフェイスで利用できるタグ付きVLANの数は限られています。10Gインターフェイスでは63個のタグ付きVLAN、1Gインターフェイスでは32個のタグ付きVLANです。VPXインスタンスは、設定されたVLAN IDを持つパケットのみを受信します。インターフェイスでVLANフィルタのステータスを無効から有効に変更した場合は、そのインターフェイスに関連付けられているVPXインスタンスを再起動してください。

VLANフィルタリングは、SDXアプライアンスでデフォルトで有効になっています。インターフェイスでVLANフィルタリングを無効にすると、そのインターフェイスで最大4096個のVLANを設定できます。

注: VLANフィルタリングは、Citrix Hypervisorバージョン6.0を実行しているSDXアプライアンスでのみ無効にできます。

インターフェイスでVLANフィルタリングを有効にするには、>をクリックします。インターフェイスを選択し、をクリックして詳細を入力し、VLANフィルタリングを有効にします。

クロック同期の構成

Network Time Protocol (NTP) 同期を有効にすると、管理サービスが再起動されます。SDXアプライアンスをNTPサーバーとローカルクロックを同期するように構成できます。その結果、SDXアプライアンスのクロックは、ネットワーク上の他のサーバーと同じ日付と時刻の設定になります。アプライアンスが再起動、アップグレード、またはダウングレードされても、クロック同期構成は変更されません。ただし、高可用性セットアップのセカンダリNetScalerインスタンスには構成が伝播されません。

NTPサーバーを追加したり、認証パラメータを変更したりすると、クロックはすぐに同期されます。NTP同期を明示的に有効または無効にすることもできます。

注: ローカルNTPサーバーがない場合は、公式NTPサイト <http://www.ntp.org>で公開されているオープンアクセスNTPサーバーのリストを見つけることができます。NetScalerをパブリックNTPサーバーを使用するように構成する前に、必ず「Rules of Engagement」ページ（すべてのパブリックタイムサーバーページに含まれるリンク）をお読みください。

NTPサーバーを構成するには、> をクリックします。

NTP同期を有効にするには

1. ナビゲーションペインで、 を展開し、 をクリックします。
2. 詳細ペインで、 をクリックします。
3. ダイアログボックスで、 を選択します。
4. 「OK」をクリックし、「閉じる」をクリックします。

認証オプションを変更するには

1. ナビゲーションペインで、 **System** を展開し、 **NTP Servers** をクリックします。
2. 詳細ペインで、 **Authentication Parameters** をクリックします。
3. 「**Modify Authentication Options**」ダイアログボックスで、次のパラメーターを設定します。

- **Authentication**—NTP認証を有効にします。指定可能な値: YES、NO。デフォルト: YES。
- **Trusted Key IDs**—信頼できるキーID。NTPサーバーを追加する際に、このリストからキー識別子を選択します。最小値: 1。最大値: 65534。
- **Revoke Interval**—Autokeyスキームで使用される特定の暗号化値の再ランダム化の間隔を、2の累乗で秒単位で指定します。デフォルト値: 17 ($2^{17}=36$ 時間)。

- **Automax Interval**—Autokeyプロトコルで使用するセッションキーリストの再生成の間隔を、2の累乗で秒単位で指定します。デフォルト値: 12 ($2^{\wedge}12=1.1$ 時間)。

4. 「OK」をクリックし、「閉じる」をクリックします。

SDXアプライアンスのプロパティを表示する

CPUコアとSSLチップの数、利用可能な合計メモリと空きメモリ、およびさまざまな製品の詳細などのシステムプロパティを、**Configuration**タブで表示します。

SDXアプライアンスのプロパティを表示するには、**Configuration**タブをクリックします。

システムリソース、ハイパーバイザー、ライセンス、およびシステムに関する次の情報を表示できます。

システムリソース:

- **総CPUコア数**: SDXアプライアンスのCPUコア数。
- **総SSLチップ数**: SDXアプライアンスの総SSLチップ数。
- **空きSSLチップ数**: インスタンスに割り当てられていないSSLチップの総数。
- **総メモリ (GB)**: アプライアンスの総メモリ (GB単位)。
- **空きメモリ (GB)**: アプライアンスの空きメモリ (GB単位)。

ハイパーバイザー情報:

- **稼働時間**: アプライアンスが最後に再起動されてからの時間 (日数、時間、分)。
- **エディション**: SDXアプライアンスにインストールされているCitrix Hypervisorのエディション。
- **バージョン**: SDXアプライアンスにインストールされているCitrix Hypervisorのバージョン。
- **iSCSI IQN**: iSCSI修飾名。
- **製品コード**: Citrix Hypervisorの製品コード。
- **シリアル番号**: Citrix Hypervisorのシリアル番号。
- **ビルド日付**: Citrix Hypervisorのビルド日付。
- **ビルド番号**: Citrix Hypervisorのビルド番号。
- **補足パック**: SDXアプライアンスにインストールされている補足パックのバージョン。

ライセンス情報:

- **プラットフォーム:** インストールされているライセンスに基づくハードウェアプラットフォームのモデル番号。
- **最大インスタンス数:** インストールされているライセンスに基づいて、SDXアプライアンスに設定できるインスタンスの最大数。
- **利用可能なインスタンス (共有):** まだ利用可能なCPUコアの数に応じて構成できるインスタンスの数。
- **最大スループット (Mbps):** インストールされているライセンスに基づいて、アプライアンスで達成できる最大スループット。
- **利用可能なスループット (Mbps):** インストールされているライセンスに基づく利用可能なスループット。

システム情報:

- **プラットフォーム:** ハードウェアプラットフォームのモデル番号。
- **製品:** NetScaler® 製品の種類。
- **ビルド:** SDXアプライアンスで実行されているNetScalerのリリースとビルド。
- **IPアドレス:** Management ServiceのIPアドレス。
- **ホストID:** Citrix HypervisorのホストID。
- **システムID:** Citrix HypervisorのシステムID。
- ****シリアル番号:** Citrix Hypervisorのシリアル番号。
- **システム時刻:** 日 月 日 時:分:秒 タイムゾーン 年 の形式で表示されるシステム時刻。
- **稼働時間:** 管理サービスが最後に再起動されてからの時間（日、時間、分単位）。
- **BIOSバージョン:** BIOSバージョン。

リアルタイムのアプライアンススループットを表示する

受信トラフィックと送信トラフィックのSDXアプライアンスの総スループットは、定期的に更新されるグラフにリアルタイムでプロットされます。デフォルトでは、受信トラフィックと送信トラフィックの両方のスループットがグラフに一緒にプロットされます。

SDXアプライアンスのスループットを表示するには、GUIで**ダッシュボード**をクリックし、****システムスループット (Mbps)****を確認します。

リアルタイムのCPUとメモリの使用状況を表示する

アプライアンスのCPUとメモリの使用状況のグラフを表示できます。グラフはリアルタイムでプロットされ、定期的に更新されます。

SDXアプライアンスのCPUとメモリの使用状況を表示するには、GUIで**ダッシュボード**をクリックし、**管理サービス統計**を確認します。

すべてのコアのCPU使用率を表示する

SDXアプライアンスの各CPUコアの使用状況を表示できます。

CPUコア使用率ペインには、次の詳細が表示されます。

- **コア番号:** アプライアンス上のCPUコア番号。
- **物理CPU:** そのコアの物理CPU番号。
- **ハイパースレッド:** そのCPUコアに関連付けられているハイパースレッド。
- **インスタンス:** そのCPUコアを使用しているインスタンス。
- **平均コア使用率:** 平均コア使用率をパーセンテージで表したもの。

SDXアプライアンスのすべてのコアのCPU使用率を表示するには、GUIで**Dashboard**をクリックし、****System CPU Usage (%)****を確認します。

SDXアプライアンスにSSL証明書をインストールする

SDXアプライアンスには、デフォルトのSSL証明書が付属しています。セキュリティ上の理由から、この証明書を独自のSSL証明書に置き換えることをお勧めします。そのためには、まずSSL証明書をManagement Serviceにアップロードし、次に証明書をインストールする必要があります。SSL証明書をインストールすると、Management Serviceとの現在のすべてのクライアントセッションが終了します。追加の構成タスクについては、Management Serviceにログインしてください。

SSL証明書をインストールするには、**System**をクリックします。**Set Up Appliance**グループで、**Install SSL Certificate**をクリックし、ウィザードに詳細を入力します。

Management ServiceでSSL証明書を表示する

Management Serviceは、安全なクライアント接続のためにSSL証明書を使用します。有効性ステータス、発行者、サブジェクト、有効期限までの日数、有効期間（開始日と終了日）、バージョン、シリアル番号など、この証明書の詳細を表示します。

SSL証明書を表示するには、**System**をクリックし、**Set Up Appliance**グループで、**View SSL Certificate**をクリックします。

NetScalerインスタンス用のSSL証明書とキー

NetScalerインスタンス用のSSL証明書とキーの個別のビューにより、使いやすさが向上します。新しいManagement ServiceノードであるSSL Certificate Filesを使用して、NetScalerインスタンスにインストールできるSSL証明書と、対応する公開鍵および秘密鍵のペアをアップロードおよび管理します。

NetScalerインスタンスのSSL証明書とキーにアクセスするには、**Configuration > NetScaler > SSL Certificate Files**に移動します。



システム設定を変更する

セキュリティ上の理由から、Management ServiceとVPXインスタンスがセキュアチャネル経由でのみ通信するように指定できます。Management Serviceのユーザーインターフェイスへのアクセスを制限することもできます。クライアントは、httpsを使用してのみManagement Serviceのユーザーインターフェイスにログオンできます。

システム設定を変更するには、**Configuration > System**をクリックし、System Settingsグループで、**Change System Settings**をクリックします。

アプライアンスの再起動

Management Serviceは、SDXアプライアンスを再起動するオプションを提供します。再起動中、アプライアンスはホストされているすべてのインスタンスをシャットダウンし、Citrix Hypervisorを再起動します。Citrix Hypervisorが再起動すると、Management Serviceとともにホストされているすべてのインスタンスが起動します。

アプライアンスを再起動するには、**Configuration > System** をクリックし、System Administrationグループで **Reboot Appliance** をクリックします。

アプライアンスのシャットダウン

Management ServiceからSDXアプライアンスをシャットダウンできます。

アプライアンスをシャットダウンするには、**Configuration > System** をクリックし、System Administrationグループで **Shut Down Appliance** をクリックします。

SDX 管理ドメイン

SDX 管理ドメイン機能は、複数の管理ドメインを作成するのに役立ちます。管理ドメインを使用して、異なる部門のリソースを分離できます。したがって、管理ドメインはリソースの制御を改善し、リソースを最適な使用のためにさまざまなドメインに分散させることができます。

SDXアプライアンスには、CPUコア、データスループット、メモリ、ディスクスペース、SSLチップ、およびプロビジョニング可能な特定の数のインスタンスなど、固定リソースが付属しています。作成できるインスタンスの数は、ライセンスによって異なります。

SDXアプライアンスは、最大3レベルの管理ドメインをサポートします。アプライアンスが出荷されると、すべてのリソースは所有者に割り当てられます。

作成する管理ドメインはすべて、所有者ドメインのサブドメインです。それぞれの場合において、サブドメインのリソースは親ドメインのリソースプールから割り当てられます。管理ドメインのユーザーは、そのドメインのリソースにアクセスできます。彼らは、同じ階層レベルの他のドメインのリソースや、自分のドメインに割り当てられていない親ドメインのリソースにはアクセスできません。ただし、親ドメインのユーザーは、そのドメインのサブドメインのリソースにアクセスできます。

サブドメインへのリソース割り当ての例

表1は、デフォルトのルートドメインのリソースを示しています。SDX管理者は、これらのリソースをサブドメインに割り当てることができます。この場合、管理者は最大で、たとえば10個のCPUコアと840GBのディスクスペースを割り当てることができます。

表1。所有者リソース

CPUコア	10
スループット (Mbps)	18500
メモリ (MB)	87300
ディスクスペース (GB)	840
SSLチップ	36
インスタンス	36

表2は、サブドメインに割り当てられたリソースを一覧表示します。そのサブドメインの名前は *Test* です。このサブドメインには、親ドメインの10個のCPUコアのうち5個が割り当てられており、残りの5個のコアは、所有者の他のサブドメインに割り当てることができます。

表2. テストドメインのリソース

CPUコア	5
スループット (Mbps)	1024
メモリ (MB)	2048
ディスク容量 (GB)	40
SSLチップ	8
インスタンス	4

サブドメインを作成する場合、*Test* ドメイン管理者は表2に記載されているリソースのみを割り当てることができます。ドメインは3レベルしか作成できないため、*Test* ドメインはサブドメインを1レベルしか持つことができません。

次の図は、表1および表2に記載されている値とは異なる値を使用して、サブドメイン間のリソース割り当ての別の例を示しています。

管理ドメインを作成するには、**Configuration > System > Administrative Domain** に移動し、必要なオプションを選択します。画面の指示に従ってください。新しいドメインが作成されたら、Management Service のログインページを使用してこのドメインにログインし、ドメイン名とユーザー名を入力します。たとえば、NewDomain という名前のドメインを NewUser というユーザーで作成した場合、NewDomain\NewUser としてログインします。

ユーザーをドメインに割り当てる

サブドメインが作成されると、管理者グループと読み取り専用グループの2つのユーザーグループが自動的に作成されます。デフォルトでは、各ユーザーは管理者グループの一部です。ユーザーは複数のグループに追加できます。

SDX 22000プラットフォームでのRAIDディスク割り当ての管理

NetScaler SDX 22040/22060/22080/22100/22120アプライアンスには、最大8台の物理ディスクをサポートできるRAID（Redundant Array of Independent Disks）コントローラーが搭載されるようになりました。複数のディスクは、パフォーマンスの向上だけでなく、信頼性の強化も提供します。SDXアプライアンスは多数の仮想マシンをホストし、ディスク障害が複数の仮想マシンに影響を与えるため、信頼性は特に重要です。管理サービス上のRAIDコントローラーは、ディスクミラーリングを実装するRAID 1構成をサポートしています。つまり、2台のディスクが同じデータを保持します。RAID 1アレイ内のディスクが故障した場合、そのミラーが直ちに必要なすべてのデータを提供します。

RAID 1ディスクミラーリングは、2台の物理ドライブを1台の論理ドライブに結合します。論理ドライブの使用可能容量は、その物理ドライブの1台の容量に相当します。たとえば、2台の1テラバイトドライブを結合すると、合計使用可能容量が1テラバイトの単一の論理ドライブが作成されます。このドライブの組み合わせは、アプライアンスには単一の論理ドライブとして表示されます。

SDXアプライアンスは、論理ドライブ0と論理ドライブ1を含む構成で出荷されます。論理ドライブ0は管理サービスとCitrix Hypervisorに割り当てられ、論理ドライブ1はプロビジョニングするNetScalerインスタンスに割り当てられます。より多くの物理ドライブを使用するには、新しい論理ドライブを作成する必要があります。

ドライブのプロパティと操作を表示する

SDXアプライアンスは、最大8つの物理ドライブスロット、つまりアプライアンスの両側に4つのスロットのペアをサポートします。物理ドライブをスロットに挿入できます。物理ドライブを使用する前に、それを論理ドライブの一部にする必要があります。

管理サービスでは、**Configuration > System > RAID**画面に、論理ドライブ、物理ドライブ、およびストレージリポジトリのタブが含まれています。

論理ドライブ

Configuration > System > RAID > Logical Drivesタブでは、各論理ドライブの名前、状態、サイズ、およびその構成物理ドライブに関する情報を表示できます。次の表は、仮想ドライブの状態について説明しています。

状態	説明
最適	仮想ドライブの動作状態は良好です。構成されているすべてのドライブがオンラインです。

状態	説明
劣化	仮想ドライブの動作状態は最適ではありません。構成されているドライブの1つが故障しているか、オフラインです。
失敗	仮想ドライブが失敗しました。
オフライン	仮想ドライブはRAIDコントローラーで利用できません。

論理ドライブを選択し、**Show Physical Drive** をクリックすることで、その論理ドライブに関連付けられている物理ドライブの詳細も表示できます。

新しい論理ドライブを作成するには

1. **Configuration > System > RAID** に移動し、**Logical Drives** タブを選択します。
2. **Add** をクリックします。
3. **Create Logical Disk** ダイアログボックスで、動作中の物理ドライブを含む2つのスロットを選択し、**Create** をクリックします。

物理ドライブ

SDXアプライアンスは最大8つの物理スロットをサポートします。これは、アプライアンスの両側に4つのスロットがペアになっていることを意味します。 **Configuration > System > RAID > Physical Drives** タブで、以下の情報を表示できます。

- **スロット:** — 物理ドライブに関連付けられている物理スロット。
- **サイズ:** — 物理ドライブのサイズ。
- **ファームウェアの状態:** — ファームウェアの状態。可能な値:
 - **オンライン、スピニング済み:** — 物理ドライブが稼働しており、RAIDによって制御されています。
 - **未構成（良好）:** — 物理ドライブは良好な状態であり、論理ドライブペアの一部として追加できます。
 - **未構成（不良）:** — 物理ドライブは良好な状態ではなく、論理ドライブの一部として追加できません。
- **外部状態:** — ディスクが空であるかどうかを示します。
- **論理ドライブ:** — 関連付けられた論理ドライブ。

物理ドライブペインでは、物理ドライブに対して次のアクションを実行できます。

- **初期化:**—ディスクを初期化します。物理ドライブが良好な状態ではなく、論理ドライブペアの一部として追加する必要がある場合に、物理ドライブを初期化できます。
- **再構築:**—ドライブの再構築を開始します。ドライブグループ内のドライブが故障した場合、故障する前にドライブに保存されていたデータを再作成することで、ドライブを再構築できます。RAIDコントローラーは、ドライブグループ内の他のドライブに保存されているデータを再作成します。
- **ドライブの特定:**—アプライアンス上のドライブを特定します。これは、ドライブに関連付けられたドライブアクティビティLEDを点滅させることで示されます。
- **ドライブの特定を停止:**—アプライアンス上のドライブの特定を停止します。
- **取り外し準備:**—選択した物理ドライブを非アクティブ化して、取り外し可能にします。

ストレージリポジトリ

Configuration > System > RAID > Storage Repositoryタブでは、SDXアプライアンス上のストレージリポジトリのステータスを表示できます。また、アタッチされていないストレージリポジトリドライブに関する情報を表示したり、そのドライブを選択して**Remove**をクリックすることで削除したりできます。**Storage Repository**タブには、各ストレージリポジトリに関する次の情報が表示されます。

- **名前:**—ストレージリポジトリドライブの名前。
- **ドライブがアタッチされているか:**—ストレージリポジトリがアタッチされているかどうか。ドライブがアタッチされていない場合は、**Remove**をクリックして削除できます。
- **サイズ:**—ストレージリポジトリのサイズ。
- **使用済み:**—使用中のストレージリポジトリスペースの量。

SDX 22000アプライアンスに論理ドライブを追加する

SDX 22000プラットフォームに追加の論理ドライブを追加するには:

1. Management Serviceにログオンします。
2. **Configuration > System > RAID**に移動します。
3. SDX 22000アプライアンスの背面で、2つの空のSSDをスロット番号4と5に挿入します。稼働中のシステムにSSDを追加できます。 **注:** SSDがNetScaler®認定済みであることを確認してください。
4. Management Serviceで、**Configuration > System > RAID**と**Physical Drives**タブに移動します。追加したSSDが表示されます。

5. **Logical Drive**タブに移動し、**Add**をクリックします。
6. **Create Logical Disk**ページで:
 - a. **First Slot**ドロップダウンリストで、4を選択します。
 - b. **Second Slot**ドロップダウンリストで、5を選択します。
 - c. **Create**をクリックします。

注: Management Serviceでは、スロット番号はゼロから始まります。そのため、Management Serviceのスロット番号付けは、物理アプライアンスのスロット番号付けとは異なります。

論理ドライブが作成され、**Logical Drive**タブの下に表示されます。更新アイコンをクリックして、論理ドライブの順序を更新します。

SDX 22000アプライアンスに2番目の論理ドライブを追加する

別の論理ドライブを追加するには、スロット番号6と7にSSDを挿入します。論理ディスクの作成ページで、最初のスロットリストから6を選択し、2番目のスロットリストから7を選択します。

故障したSSDドライブを空のSSDドライブと交換する

故障したSSDドライブを空のSSDドライブと交換するには：

1. **構成 > システム > RAID** に移動します。
2. 「**物理ドライブ**」タブで、交換する故障したドライブを選択します。
3. 「**取り外し準備**」をクリックしてドライブを取り外します。
4. 更新アイコンをクリックして、物理ドライブのリストを更新します。
5. 故障したドライブをスロットから物理的に取り外します。
6. 故障したSSDを取り外したスロットに、新しいCitrix®検証済みSSDを挿入します。
7. Management Serviceで、**構成 > システム > RAID** に移動します。新しいSSDは「**物理ドライブ**」セクションに表示されます。ドライブの再構築プロセスが自動的に開始されます。

更新アイコンをクリックして、再構築プロセスのステータスを確認します。再構築プロセスが完了すると、**ファームウェアの状態列**に「オンライン、スピニングアップ」ステータスが表示されます。

SDXライセンスの概要

重要:

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきましたが、April 15, 2026にサポート終了（EOL）となります。ライセンスアクティベーションサービス（LAS）は、Citrix製品スイート全体で製品アクティベーションを行うための次世代テクノロジーです。April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法はLASとなり、NetScaler Flexedライセンス（CPL/UHMC）、レガシーなNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

注: Console on-premのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026以降、Console on-premリリース14.1-51.x以降および13.1-60.x以降で非推奨となります。Console on-premリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026までにConsole on-premリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、永続ライセンスなど、その他のレガシーなNetScalerライセンスはLASではサポートされません。アクティブなメンテナンスがない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスなしの状態になります。

LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。

ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件の不遵守に対し、Citrixが法律上または衡平法上持つ可能性のあるその他の救済措置に加

えて、責任を負うことなくCitrixメンテナンスを制限または停止する場合があります。これらの要件は、法律または規制によって禁止されている場合には適用されません。

ライセンスアクティベーションサービス

ライセンスアクティベーションサービス（LAS）は、従来のファイルベースのライセンスに代わる新しいクラウドベースのライセンスソリューションです。LASは、CitrixおよびNetScaler製品のアクティベーション用の新しいモジュールを導入し、シームレスで最新のライセンス管理アプローチを保証します。

注:

LASはライセンスメカニズムであり、ライセンスタイプではありません。

詳細については、「[License Activation Service](#)」を参照してください。

SDXアプライアンスでのライセンスの管理

注:

ライセンスの詳細については、NetScaler SDX Management Serviceのユーザーインターフェイスを参照してください。

NetScaler SDX Management Serviceでは、ハードウェアシリアル番号（HSN）またはライセンスアクセスコードを使用してライセンスを割り当てることができます。Management Serviceソフトウェアは、アプライアンスのシリアル番号を内部的に取得し、Citrixはライセンス購入時にライセンスアクセスコードをメールで送信します。

または、ライセンスがローカルコンピューターにすでに存在する場合は、それをアプライアンスにアップロードできます。

ライセンスの返却や再割り当てなど、その他のすべての機能については、ライセンスポータルを使用する必要があります。オプションで、ライセンス割り当てにライセンスポータルを使用することもできます。詳細については、「[Manage Licenses on citrix.com](#)」を参照してください。

SDXライセンスオプションの詳細については、以下を参照してください。

- [適切なプラットフォームとエディションのオプションの選択。](#)
- [ライセンスモデル](#)

注：永続ライセンスまたはプールライセンスのインストールには、SDXアプライアンスの再起動は必要ありません。

前提条件

ハードウェアシリアル番号またはライセンスアクセスコードを使用してライセンスを割り当てるには：

1. アプライアンスを介してパブリックドメインにアクセスできる必要があります。たとえば、アプライアンスはwww.citrix.comにアクセスできる必要があります。ライセンス割り当てソフトウェアは、内部的にCitrixライセンスポータルにアクセスしてライセンスを取得します。パブリックドメインにアクセスするには、Management Service IPアドレスを設定し、DNSサーバーをセットアップする必要があります。
2. ライセンスはハードウェアにリンクされているか、有効なライセンスアクセスコードが必要です。

Management Service を使用したライセンスの割り当て

ライセンスがすでにハードウェアにリンクされている場合、ライセンス割り当てプロセスでハードウェアのシリアル番号を使用できます。そうでない場合は、ライセンスアクセスコードを入力する必要があります。

展開の要件に応じて、ライセンスを部分的に割り当てることができます。たとえば、ライセンスファイルに10個のライセンスが含まれていても、現在の要件が6個のライセンスのみである場合、今すぐ6個のライセンスを割り当て、後でさらにライセンスを割り当てることができます。ライセンスファイルに存在するライセンスの総数を超えるライセンスを割り当てることはできません。

ライセンスを割り当てるには

1. Webブラウザで、SDXアプライアンスのManagement ServiceのIPアドレスを入力します (例: `<http://10.102.126.251>`)。
2. ユーザー名とパスワードに、管理者資格情報を入力します。
3. **Configuration** タブで、**System > Licenses** に移動します。
4. 詳細ペインで、**Add License File** をクリックします。



5. 次に、次のいずれかのオプションを選択します。

- ローカルコンピューターからライセンスファイルをアップロードする (このオプションはデフォルトで選択されています)

- ライセンスアクセスコードを使用する
- ハードウェアのシリアル番号を使用する



- **ローカルコンピューターからライセンスファイルをアップロード:** このオプションを選択した場合、**参照**をクリックしてローカルマシンからゼロキャパシティライセンスを選択します。その後、**完了**をクリックします。
 - ゼロキャパシティライセンスが正常に適用されると、**ライセンスページにライセンスモードセクション**が表示されます。
 - プールライセンスまたはセルフマネージドプールライセンス**のいずれかを選択できます。
 - ライセンスサーバー名またはIPアドレスフィールド**に、ライセンスサーバーの詳細を入力します。
 - ポート番号フィールド**に、ライセンスサーバーのポートを入力します。デフォルト値: 27000。
 - ライセンスの取得**をクリックします。
 - ライセンスの割り当て**ウィンドウで、必要なインスタンスと帯域幅を指定し、**割り当て**をクリックします。
 - ライセンスの管理**ページで、ライセンスサーバー、ライセンスエディション、およびプールから割り当てられたインスタンスと帯域幅の詳細を表示できます。

注:

NetScalerリリース13.1ビルド30.x以降、NetScaler SDXアプライアンスはセルフマネージドプールライセンスをサポートしています。このライセンスを使用すると、ライセンスサーバーへのライセンスファイルのアップロードを簡素化および自動化できます。NetScaler Consoleを使用して、共通の帯域幅またはvCPUとインスタンスプールで構成されるライセンスフレームワークを作成できます。

- **ライセンスアクセスコードを使用:** このオプションを選択した場合、**ライセンスアクセスコードフィールド**に**LAC**を入力するか、プロキシサーバー経由で接続するためのチェックボックスを選択します。次に、**ライセンスの取得**をクリックします。
 - ライセンスを割り当てるために使用するライセンスファイルを選択します。
 - **割り当て**列に、割り当てるライセンスの数を入力します。次に、**ダウンロード**をクリックします。

ライセンスがダウンロードされると、**ライセンスファイル**の下に表示されます。ライセンスファイルを選択し、**ライセンスの適用**をクリックします。

- **ハードウェアシリアル番号を使用**: このオプションを選択した場合、ソフトウェアは内部的にアプライアンスのシリアル番号を取得し、この番号を使用してライセンスを表示します。
 - 「**ライセンスの取得**」をクリックするか、「**プロキシサーバー経由で接続**」のチェックボックスをオンにしてから「**ライセンスの取得**」をクリックします。

ライセンスファイルをダウンロードしたら、ライセンスファイルを選択し、「**ライセンスの適用**」をクリックします。

プールライセンスの詳細については、「NetScaler SDX の永続ライセンスを NetScaler プール容量にアップグレードする」([/ja-jp/citrix-application-delivery-management-software/current-release/license-server/adc-pooled-capacity/upgrade-perpetual-license-sdx-pooled-capacity.html](https://ja-jp.citrix-application-delivery-management-software/current-release/license-server/adc-pooled-capacity/upgrade-perpetual-license-sdx-pooled-capacity.html)) を参照してください。

ライセンスの有効期限とデータトラフィック処理の制限

NetScaler リリース 14.1-38.x 以降、SDX プールライセンスの有効期限が切れると、VPX インスタンスのスループットは直ちに 20 Mbps に制限されます。この機能は、NetScaler 14.1-43.x 以降のプールライセンスと固定ライセンスの両方で利用できます。ただし、NetScaler 14.1-38.x では、プールライセンスでのみ利用可能です。

ユーザーは、> で、プールライセンスまたはフレックスライセンスの有効期限が切れるまでの残り日数を確認できます。この情報は 24 時間ごとに更新されます。システムは有効期限の 30 日前に有効期限をチェックし、ライセンスが更新されるまで 24 時間ごとに更新アラートを送信します。

SDX ライセンスの有効期限が切れると、Management Service は、関連する VPX インスタンスのスループットを 20 Mbps に制限します。この制限は、Management Service の再起動を必要とせずに、直ちに有効になります。以前は、この制限は Management Service の再起動後にのみ有効になり、スループットは 1 Mbps に削減されていました。

ライセンスアクティベーションサービス

重要:

従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、April 15, 2026にサポート終了（EOL）となります。License Activation Service (LAS) は、Citrix製品スイート全体にわたる製品アクティベーションのための次世代テクノロジーです。April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法はLASになり、NetScaler Flexedライセンス (CPL/UHMC)、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポート
- NetScaler Console オンプレミス版：14.1-51.x

注: Console on-prem のLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026をもって、Console on-prem リリース14.1-51.x以降および13.1-60.x以降では非推奨となります。Console on-prem リリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026までにConsole on-prem リリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、Perpetualなどの他のすべての従来のNetScalerライセンス形式は、LASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。

LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。

ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrix® は、これらの要件を遵守しない場合、Citrix が法律または衡平法上持つその他の救済措置に加えて、責任

を負うことなく Citrix Maintenance を制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。

LASへの移行を開始する前に、[LAS for NetScaler](#) を読むことをお勧めします。これにより、一般的な前提条件、サポートされているライセンスタイプまたはサポートされていないライセンスタイプ、特定のライセンスおよび展開タイプに対する正確なワークフロー、およびその他の重要な情報を確実に理解できます。

LASは、従来のファイルベースのライセンスに代わる、新しいクラウドベースのライセンスソリューションです。LASは、CitrixおよびNetScaler製品のアクティベーションのための新しいモジュールを導入し、ライセンス管理に対するシームレスで最新のアプローチを保証します。

注:

LASはライセンスメカニズムであり、ライセンスタイプではありません。LASはNetScaler展開向けの固定期間帯域幅ライセンスをサポートしています。永続ライセンスなど、従来のNetScalerライセンスの他のすべての形式はLASではサポートされていません。

LASのNetScalerバージョン互換性

LASを使用するには、NetScalerで次の最小バージョン以降が実行されている必要があります。

- **NetScaler ADC:** 14.1ビルド51.80、13.1ビルド60.29、13.1ビルド37.247 (FIPS)
- **Management Service (NetScaler SVM):** 14.1ビルド51.83、13.1ビルド60.30

注:

SDXアプライアンスの場合、Management Service (SVM) をLASでサポートされているビルドにアップグレードし、LASベースのライセンスに移行してください。VPXビルドバージョンはLASの互換性に影響しません。

前提条件

LASを使用するには、次の前提条件を完了していることを確認してください。

- 有効なCitrix Cloudアカウントが必要です。既存のクラウドアカウントの詳細、または新しいクラウドアカウントのオンボーディングについては、「[アカウント管理](#)」を参照してください。
- LASアクティベーションワークフローに使用されるCitrix Cloudアカウントにリンクされている組織ID (Org ID) は、有効な購入済みエンタイトルメントを所有する必要があります。現在のエンタイトルメントを表示するには、「[エンタイトルメント](#)」を参照してください。

- NetScalerがLAS互換バージョンで実行されていることを確認してください。

NetScaler GUIを使用したLASへの移行

次のいずれかの場合は、このセクションで説明する手順に従ってください。

- ファイルベースのライセンスを使用しており、固定期間帯域幅LASベースのライセンスに移行する固定期間帯域幅のお客様。
- ライセンスのないNetScalerを所有しており、固定期間帯域幅LASベースのライセンスを使用したい場合。
- ファイルベースのライセンスを使用している永続ライセンスのお客様が、固定期間帯域幅LASベースのライセンスに移行する場合。

ステップ1: NetScaler GUIで、**System > Licenses** に移動し、**LAS Offline Activation** オプションを選択します。

LASオフラインアクティベーション(/en-us/sdx/media/las-offline-activation.png)

ステップ2: LASアクティベーションは、特定のNetScaler SDXインスタンスの一意的ID情報を含むアクティベーション要求ファイルを生成することから始まります。

1. LASアクティベーション要求ファイルを生成するには、**Generate NetScaler SDX activation request** セクションで、**Generate** をクリックします。

NetScalerオフラインアクティベーション要求ファイルの生成(/en-us/sdx/media/generate-offline-request-file.png)

2. アクティベーション要求ファイルが生成されたら、**Download** をクリックしてローカルシステムに保存します。

注:

アクティベーション要求ファイルは7日後に期限切れになります。ファイルが有効なままであることを確認するために、この期間内に**ステップ3**で説明されているアクティベーションプロセスを完了してください。

NetScalerオフラインアクティベーション要求ファイルのダウンロード(/en-us/sdx/media/download-activation-request-file.png)

ステップ3: **ステップ2**で生成されたアクティベーション要求ファイルをCitrix Cloud™ (LAS UI) にアップロードして、NetScalerのライセンスアクティベーションファイルまたはプロブを生成します。

1. Citrix Cloudにログインし、**Citrix Cloud > Licensing > NetScaler licenses > NetScaler SDX** に移動します。
2. **ステップ2**で生成されたアクティベーション要求ファイルをアップロードします。
3. ファイルが正常にアップロードされたら、NetScalerに必要なライセンスタイプを選択します。

注記:

複数のFixed-term Bandwidthエンタイトルメントがある場合、ドロップダウンメニューに利用可能なすべてのエンタイトルメントが表示されます。このNetScalerインスタンスに適切なものを選択してください。

4. ライセンスの種類を選択したら、ライセンスアクティベーションファイルを生成してダウンロードします。

注記:

ライセンスアクティベーションファイルは、生成から1年間有効です。



ステップ4: NetScaler GUIに戻り、**System > Licenses** に移動して、**LAS Offline Activation** オプションを選択します。

1. **Upload NetScaler SDX activation file** セクションで、**Upload File** をクリックして、**ステップ3**で生成されたライセンスアクティベーションファイルをアップロードします。



2. アクティベーションファイルをアップロードしたら、**Yes** をクリックしてアクティベーションを確認します。



ステップ5: これで、NetScaler SDXはLASを通じてライセンスが付与されました。



ステップ6: 継続的な運用を確保するために、ライセンスアクティベーションファイルを監視および管理します。

ライセンスアクティベーションファイルは1年間有効です。インターフェイスで、最終更新日またはアクティベーション日と、次の更新日またはアクティベーション日の両方を確認できます。

NetScalerの機能を継続的に維持するには、次の更新期限が切れる前に「**今すぐ更新**」をクリックし、**ステップ2**から**ステップ5**を繰り返します。

LASを更新(/en-us/sdx/media/las-renewal-date.png)

重要:

ライセンスアクティベーションファイルまたはプロブを期限内に更新して適用しない場合、NetScalerはライセンスなしの状態になります。

ステップ7: Citrix Cloudにログインし、**Licensing > NetScaler licenses > NetScaler SDX**に移動して、LASアクティベーションプロブを表示します。

注:

デフォルトでは、LASはシステム識別子 (`lsguid`) を使用して、アクティベーションプロブのリスト表示のためにNetScalerの展開を識別します。

システム識別子 (`lsguid`) の代わりにホスト名が選択されている場合、ホスト名が**NetScaler GUI**フィールドに表示されます。

ホスト名(/en-us/sdx/media/sdx_hostname.png)

注:

LASへの移行が完了したら、SVM上のローカルファイルベースライセンスを削除します。ファイルベースライセンスはSVMフォルダー `/mpsconfig/license` にあり、シェルプロンプトを使用してこのフォルダーから削除する必要があります。

ライセンスアクティベーションファイルの動作と有効期限

ライセンスアクティベーションファイルまたはプロブは、生成日から1年間有効です。お客様は、次の更新日を追跡し、有効期限が切れる前にファイルを更新する責任があります。

重要:

ライセンスアクティベーションファイルを有効期限前に更新しなかった場合、NetScalerはライセンスなしの状態になります。

ライセンス契約の有効期限

ライセンス契約の有効期限が切れるまでの残り日数は、**System > Licenses > LAS offline activation** に移動すると、**License Entitlement Expiry** の下に表示されます。

ライセンスエンタイトルメントの有効期限(/en-us/sdx/media/las-license-entitlement-expiry.png)

NetScalerがスムーズに機能するように、ライセンス契約の有効期限が切れる前に、ライセンス契約を更新し、[NetScaler GUI を使用したLASへの移行](#)セクションに記載されている手順を完了する必要があります。

重要

- ライセンス契約が期限内に更新されない場合、NetScalerはライセンスなしの状態になります。
- ライセンスの有効期限が切れると、NetScalerインスタンスは通常の動作を停止し、設定の損失やトラフィック処理の完全なシャットダウンなどが含まれます。

LASライセンスワークフロー中にLASに送信される情報

このセクションでは、すべての初期リクエストおよび各LASアクティベーションプロブ更新リクエスト中に、アクティベーションプロブのLASへのリクエストの一部として送信されるすべての情報について詳しく説明します。

次の表は、ライセンスワークフロー中にLASに送信されるパラメータをまとめたものです。

パラメータ	説明	LASワークフローにおける必要性
タイプ	オフラインNetScalerのLAS展開タイプを識別するためにハードコードされています。	LAS側での追跡用
lsguid/lxid	NetScalerの一意のID	LASバインディングパラメータ
NSIPとホスト名	IP_hostname形式のNetScalerの現在のホスト名	LAS側での追跡用
エルエスビルド	NetScalerのバージョンとビルド	LAS側での追跡用

パラメータ	説明	LASワークフローにおける必要性
リクエスト時間	リクエストパッケージ (<code>tgz</code>) が作成されたときのタイムスタンプ	LASバインディングパラメータ
組織ID	顧客の組織ID	LASバインディングパラメータ
シーシーアイディー	顧客のCC ID	LASバインディングパラメータ
プラットフォーム	NetScalerのフォームファクターとモデル	LASバインディングパラメータ
バーンイン日付	NetScalerのバージョンとビルドのソフトウェアリリース日	LAS側での追跡用
最終アクティベーションID	更新時に送信された以前のLASアクティベーションID	LASバインディングパラメータ
UIバージョン	ファイルの整合性検証を保証します	ファイル整合性検証

LASアクティベーション識別子の設定

NetScaler ADCまたはManagement Service (SVM) 14.1-60.57、NetScaler ADCまたはManagement Service 13.1-61.26、およびNetScaler FIPS 13.1-37.259以降、NetScaler (ADCまたはManagement Service) の展開におけるLASベースのライセンスワークフローでは、IPアドレスとホスト名は使用されなくなりました。代わりに、LASはシステム識別子 (`lsguid`) を使用して、NetScaler (ADCまたはManagement Service) の展開を一意に識別します。

システム識別子 (`lsguid`) の代わりにホスト名を使用するには、NetScaler GUIから**Use hostname for LAS activation blob workflow**オプションを手動で選択します。

LASアクティベーションのホスト名を有効にするには

1. **System > Licenses > LAS Activation**に移動します。
2. **Use hostname for LAS activation blob workflow**トグルをオンにします。

ホスト名のアクティベーション(/en-us/sdx/media/las-sdx.png)

LAS移行済みNetScaler SDX (SVM) を監視するためのベストプラクティス

このセクションでは、NetScaler SDX (SVM) でLASを使用しており、Fixed Capacity Subscription ライセンスタイプをお持ちの場合に、NetScaler SDXを監視するために従うことができるベストプラクティスについて詳しく説明します。

前提条件

- [NetScaler用LAS](#) ページを読み、NetScaler SDX (SVM) でのLASに関するFAQを含めてください。
- [ライセンスアクティベーションサービス](#) を読み、LAS移行を完了してください。
- 関連する通知を設定し、NetScaler SDX (SVM) のGUIとCLIを定期的に監視するようにしてください。

注:

通知の継続的な改善を行い、このドキュメントもそれに応じて更新していく予定です。

LASアクティベーションプロブの有効期限の監視

SVM GUIとCLIを使用して、LASアクティベーションプロブの有効期限を追跡し、予期せぬライセンス中断を回避できます。

SVM GUI:

SVM GUI > Configuration > System > Licenses > LAS Offline Activation > ADC Licenses に移動し、**今後の更新** を監視します。



SVM CLI:

`show license` コマンドを使用し、`Expiry Days` パラメータの値を参照できます。

サンプル:

```
show license
```

```
Platform: 9120
```

```
Cluster: false

Maximum Instances: 4

Available Instances: 4

Maximum Throughput (Mbps): 20000

Available Throughput (Mbps): 20000

isPooledLicense: false

Expiry Days: 208

isLASLicense: false

isLASFixedLicense: true

Done
```



通知

SVM GUI上のバナー:

このGUIバナーは、LASアクティベーションプロブの有効期限が30日以内に迫っている場合、NetScaler SDXインスタンスによってデフォルトでトリガーされます。ユーザーがログインするたびにGUIに表示されます。



SNMPベースの通知

SNMPトラップまたはアラームは、有効期限が迫っている場合は `LicenseExpiry`、すでに期限切れの場合は `LicenseExpired` と名付けられています。

SNMPトラップ `LicenseExpiry` は、LASアクティベーションプロブの有効期限が30日以内に迫っている場合、NetScaler SDXインスタンスによってデフォルトでトリガーされます。このトラップは、LASアクティベーションプロブの有効期限の30日前から24時間ごとに生成され、プロブが期限切れになるまで継続されます。

SDX/SVMのSNMPトラップ宛先を設定する必要があります。設定が完了すると、これらのSNMPトラップを受信します。

サンプル:

```
[EventNotification[#1]] Inside: send_ns_snmp_trap_LicenseExpiry
```



System > Eventsに移動して、生成されたイベントを表示できます。表示されるメッセージは、「LASアクティベーションプロブは **d** 日以内に期限切れになります」です。

**ライセンスエンタイトルメントの有効期限の監視 (契約の有効期限)****SVM GUI:**

SVM GUI > Configuration > System > Licenses > LAS Offline Activation > ADC Licenses に移動し、ライセンスエンタイトルメントの有効期限を監視します。

ライセンスエンタイトルメントの有効期限(/en-us/sdx/media/sdx-las-bp-entitlement-expiry.png)

通知**SVM GUI のバナー:**

SVM GUI のこのバナーは、ライセンスエンタイトルメントの有効期限が30日以内に迫っている場合に、NetScaler SDX インスタンスによってトリガーされます。これは、ユーザーがログインするたびにGUIに表示されます。

ライセンス有効期限GUIバナー(/en-us/sdx/media/sdx-las-bp-expiry-banner.png)

SNMPベースの通知:

NetScaler SDX は、ライセンスエンタイトルメントの有効期限に関するイベントを生成します。

SNMPトラップまたはアラームは、期限切れが迫っている場合は **LicenseExpiry**、すでに期限切れの場合は **LicenseExpired** と名付けられています。

SNMPトラップ **LicenseExpiry** は、ライセンスエンタイトルメントの有効期限が30日以内に迫っている場合に、NetScaler SDX インスタンスによってデフォルトでトリガーされます。このトラップは、ライセンスエンタイトルメントの有効期限の30日前から、期限切れになるまで24時間ごとに生成されます。

SDX/SVM の SNMP トラップ宛先を設定する必要があります。設定が完了すると、これらの SNMP トラップを受信します。

これらのイベントを表示するには、**SDX GUI > System > Events** に移動します。表示されるメッセージは、「ライセンスエンタイトルメントは **x** 日で期限切れになります」（最新ビルド）または「ライセンスは **x** 日で期限切れになります」（一部の古いビルド）です。

システムイベント(/en-us/sdx/media/sdx-las-bp-system-events.png)

SDX リソースビジュアライザー

NetScaler SDXアプライアンスにNetScalerインスタンスがプロビジョニングされると、CPU、スループット、メモリなどの様々なリソースをインスタンスに割り当てる必要があります。現在のSDXでは、利用可能な様々なリソースに関する情報は表示されません。

リソースビジュアライザーを使用すると、インスタンスのプロビジョニングに使用できるすべての利用可能なリソースが、単一のダッシュボードに表示されます。利用可能なリソースと使用中のリソースはすべてグラフィカルな形式で表示されます。リソースビジュアライザーは、割り当て可能なリソースとは別に、電源ステータスや温度などの他のパラメータも表示します。

リソースビジュアライザーは、インスタンスが使用している様々なリソースも表示します。インスタンスに関連付けられている様々なリソースを表示するには、ビジュアライザーでインスタンス名をクリックします。ビジュアライザーの右側には、利用可能なリソースと使用中のリソースがすべてグラフィカルな形式で表示されます。

次の図は、リソースビジュアライザーで取得された詳細を示しています。



インターフェースを管理する

インターフェースペインでは、VPXインスタンス上の仮想インターフェースとSDXアプライアンスのマッピングを表示し、インターフェースにMACアドレスを割り当てることができます。

注: ダイレクトアタッチケーブル (DAC) が接続されているインターフェースでは、オートネゴシエーションはサポートされていません。

インターフェースペインのインターフェースリストの**状態列**で、UPはインターフェースが正常にトラフィックを受信していることを示します。DOWNは、インターフェースがトラフィックを送受信できないネットワークの問題を示します。

重要: 1 GBを超える接続からのフロー制御は推奨されません。

インターフェースを構成するには

1. **構成**タブのナビゲーションペインで、システムを展開し、**インターフェース**をクリックします。
2. **インターフェース**ペインで、構成するインターフェースをクリックし、**編集**をクリックします。
3. **インターフェースの構成**ウィンドウで、次のパラメータの値を指定します。
 - **オートネゴシエーション** — オートネゴシエーションを有効にします。指定可能な値: ON、OFF。デフォルト: ON。
 - **速度** — インターフェースのイーサネット速度 (Mb/秒)。指定可能な値: 10、100、1000、10000。
 - **デュプレックス** — インターフェースのデュプレックス動作のタイプ。指定可能な値: Full、Half、NONE。デフォルト: NONE。
 - **フロー制御オートネゴシエーション** — フロー制御パラメータを自動的にネゴシエートします。指定可能な値: ON、OFF。デフォルト: ON。
 - **Rxフロー制御** — Rxフロー制御を有効にします。指定可能な値: ON、OFF。デフォルト: ON。
 - **Txフロー制御** — Txフロー制御を有効にします。指定可能な値: ON、OFF。デフォルト: ON。
4. 「**OK**」をクリックし、次に「**Close**」をクリックします。

インターフェイスのパラメータをデフォルト値にリセットするには

1. **Configuration**タブのナビゲーションペインで、**System**を展開し、**Interfaces**をクリックします。
2. **Interfaces**ペインで、リセットするインターフェイスをクリックし、**Reset**をクリックします。

VPXインスタンス上の仮想インターフェイスと物理インターフェイスのマッピングを表示する

NetScaler VPXインスタンスでは、GUIとCLIに、インスタンス上の仮想インターフェイスとアプライアンス上の物理インターフェイスのマッピングが表示されます。

VPXインスタンスにログオンした後、構成ユーティリティで**Network**に移動し、**Interfaces**をクリックします。インスタンス上の仮想インターフェイス番号と、アプライアンス上の対応する物理インターフェイス番号が、次の図に示すように**Description**フィールドに表示されます。

CLIで、 `show interface` コマンドを入力します。例：

```
> show interface

1) Interface 10/3 (10G VF Interface, PF 10/4) #2

flags=0xe460 <ENABLED, UP, UP, HAMON, 802.1q>

MTU=1500, native vlan=1, MAC=6e:b6:f5:21:5d:db, uptime 43h03m35s

Actual: media FIBER, speed 10000, duplex FULL, fctl NONE, throughput 10000

RX: Pkts(2547925) Bytes(287996153) Errs(0) Drops(527183) Stalls(0)

TX: Pkts(196) Bytes(8532) Errs(0) Drops(0) Stalls(0)

NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)

Bandwidth thresholds are not set.

...
```

インターフェイスへのMACアドレスの割り当て

SDXアプライアンスでADCインスタンスをプロビジョニングすると、Citrix Hypervisor™は、そのインスタンスに関連付けられた仮想インターフェイスにMACアドレスを内部的に割り当てます。同じMACアドレスが、同じアプライアンスまたは別のアプライアンス上の別のインスタンスに関連付けられた仮想インターフェイスに割り当てられる場合があります。重複するMACアドレスの割り当てを防ぐために、一意のMACアドレスを強制できます。

インターフェイスにMACアドレスを割り当てる方法は2つあります。

1. ベースMACアドレスと範囲をインターフェイスに割り当てる：管理サービスは、ベースアドレスと範囲を使用して一意のMACアドレスを割り当てます。
2. グローバルベースMACアドレスを割り当てる：グローバルベースMACアドレスはすべてのインターフェイスに適用されます。管理サービスは、すべてのインターフェイスのMACアドレスを生成します。グローバルベースMACアドレスを設定すると、1Gインターフェイスの範囲は8に設定されます。10Gインターフェイスの範囲は64に設定されます。グローバルベースMACアドレスが00:00:00:00:00:00に設定されている場合のサンプルベースMACアドレスについては、次の表を参照してください。

物理インターフェイス	ベースMACアドレス
0/1	00:00:00:00:00:00
0/2	00:00:00:00:00:08
1/1	00:00:00:00:00:10
1/2	00:00:00:00:00:18
1/3	00:00:00:00:00:20
1/4	00:00:00:00:00:28
1/5	00:00:00:00:00:30
1/6	00:00:00:00:00:38
1/7	00:00:00:00:00:40
1/8	00:00:00:00:00:48
10/1	00:00:00:00:00:50
10/2	00:00:00:00:00:90

表1. グローバルベースMACアドレスから生成されたベースMACアドレスの例

管理ポートのベースMACアドレスは参照用です。管理サービスは、ベースMACアドレスに基づいて、1/xおよび10/xポートのみのMACアドレスを生成します。

注: チャンネルにベースMACアドレスを割り当てることはできません。

MACアドレスに関するさまざまな操作を実行するには、**System > Interfaces** をクリックします。インターフェイスを選択し、**Edit** をクリックします。**Configure Interface** ウィンドウでMACアドレス操作を実行します。

SDXアプライアンスの物理インターフェイスを無効または有効にする

SDXアプライアンスの物理インターフェイスを使用していない場合は、管理サービスを使用して物理インターフェイスを無効にできます。この操作はセキュリティ目的で役立ちます。

注: デフォルトでは、SDXアプライアンスのすべての物理インターフェイスが有効になっています。また、インターフェイスがVPXまたはチャンネルで使用されている場合、そのインターフェイスを無効にすることはできません。

物理インターフェイスを無効にするには:

1. **Configuration**タブで、ナビゲーションペインの**System**を展開し、**Interfaces**をクリックします。
2. **Interfaces**ペインで、無効にするインターフェイスを選択します。
3. **Action**ドロップダウンリストで、**Disable**をクリックします。

無効になっている物理インターフェイスを使用する場合は、Management Serviceを使用してインターフェイスを有効にできます。

無効になっている物理インターフェイスを有効にするには:

1. **Configuration**タブで、ナビゲーションペインの**System**を展開し、**Interfaces**をクリックします。
2. **Interfaces**ペインで、有効にする無効なインターフェイスを選択します。
3. **Action**ドロップダウンリストで、**Enable**をクリックします。

SDXアプライアンスでのジャンボフレーム

NetScaler SDXアプライアンスは、最大9216バイトのIPデータを含むジャンボフレームの受信および送信をサポートします。ジャンボフレームは、標準の1500バイトのIP MTUサイズで可能な場合よりも、より効率的に大きなファイルを転送できます。

NetScaler SDXアプライアンスは、次の展開シナリオでジャンボフレームを使用できます。

- **ジャンボからジャンボ:** アプライアンスはジャンボフレームとしてデータを受信し、ジャンボフレームとして送信します。
- **非ジャンボからジャンボ:** アプライアンスは非ジャンボフレームとしてデータを受信し、ジャンボフレームとして送信します。
- **ジャンボから非ジャンボ:** アプライアンスはジャンボフレームとしてデータを受信し、非ジャンボフレームとして送信します。

SDXアプライアンスにプロビジョニングされたNetScalerインスタンスは、次のプロトコルに対するロードバランシング構成でジャンボフレームをサポートします。

- TCP

- TCP上のその他のプロトコル
- SIP

ジャンボフレームの詳細については、ユースケースを参照してください。

ユースケース: ジャンボからジャンボへのセットアップ

NetScalerインスタンスNS1で構成されたSIPロードバランシング仮想サーバーLBVS-1が、サーバーS1とS2間でSIPトラフィックをロードバランシングするために使用される、ジャンボからジャンボへのセットアップの例を考えてみましょう。クライアントCL1とNS1間の接続、およびNS1とサーバー間の接続はジャンボフレームをサポートします。

NS1のインターフェース10/1は、クライアントCL1からのトラフィックを受信または送信します。NS1のインターフェース10/2は、サーバーS1またはS2からのトラフィックを受信または送信します。NS1のインターフェース10/1と10/2は、それぞれVLAN 10とVLAN 20の一部です。

ジャンボフレームをサポートするために、インターフェース10/1、10/2、およびVLAN 10、VLAN 20に対してMTUは9216に設定されます。

このセットアップ例では、CL1、S1、S2を含む他のすべてのネットワークデバイスも、ジャンボフレームをサポートするように構成されています。

ジャンボ-ジャンボ(/en-us/sdx/media/jumbo_to_jumbo.png)

次の表に、この例で使用されている設定を示します。

エンティティ	名前	詳細
クライアントCL1のIPアドレス	CL1	192.0.2.10
サーバーのIPアドレス	S1	198.51.100.19
	S2	198.51.100.20
インターフェース（管理サーバーインターフェースを使用）およびNS1上のVLAN（CLIを使用）に指定されたMTU。	10/1	9000
	10/2	9000

エンティティ	名前	詳細
	VLAN 10	9000
	VLAN 20	9000
NS1上のサーバーを表すサービス	SVC-S1	IPアドレス: 198.51.100.19; プロトコル: SIP; ポート: 5060
NS1上のサーバーを表すサービス	SVC-S2	IPアドレス: 198.51.100.20; プロトコル: SIP; ポート: 5060
VLAN 10上のロードバランシング仮想サーバー	LBVS-1	IPアドレス: 203.0.113.15; プ ロトコル: SIP; ポート: 5060;SVC-S1, SVC-S2

CL1からNS1へのリクエストのトラフィックフローは次のとおりです。

1. CL1はLBVS1に対して20000バイトのSIPリクエストを作成します。
2. CL1は、リクエストデータをIPフラグメントでNS1のLBVS1に送信します。各IPフラグメントのサイズは、CL1がこれらのフラグメントをNS1に送信するインターフェイスに設定されたMTU (9000) 以下です。
 - 最初のIPフラグメントのサイズ === 9000
 - 2番目のIPフラグメントのサイズ === 9000
 - 最後のIPフラグメントのサイズ === 2068
3. NS1はインターフェイス10/1でリクエストIPフラグメントを受信します。NS1はこれらのフラグメントを受け入れます。これは、各フラグメントのサイズがインターフェイス10/1のMTU (9000) 以下であるためです。
4. NS1はこれらのIPフラグメントを再構成して27000バイトのSIPリクエストを形成します。NS1はこのリクエストを処理します。
5. LBVS-1の負荷分散アルゴリズムはサーバーS1を選択します。
6. NS1はリクエストデータをIPフラグメントでS1に送信します。各IPフラグメントのサイズは、NS1がこれらのフラグメントをS1に送信するインターフェイス10/2のMTU (9000) 以下です。IPパケットはNS1のSNIPアドレスを送信元とします。
 - 最初のIPフラグメントのサイズ === 9000

- 2番目のIPフラグメントのサイズ === 9000
- 最後のIPフラグメントのサイズ === 2068

この例における、S1からCL1への応答のトラフィックフローは次のとおりです。

1. サーバーS1は、NS1のSNIPアドレスに送信するために30000バイトのSIP応答を作成します。
2. S1は応答データをIPフラグメントでNS1に送信します。各IPフラグメントのサイズは、S1がこれらのフラグメントをNS1に送信するインターフェイスに設定されているMTU（9000）以下です。

- 最初のIPフラグメントのサイズ === 9000
- 2番目と3番目のIPフラグメントのサイズ === 9000
- 最後のIPフラグメントのサイズ === 3088

3. NS1はインターフェイス10/2で応答IPフラグメントを受信します。各フラグメントのサイズがインターフェイス10/2のMTU（9000）以下であるため、NS1はこれらのフラグメントを受け入れます。
4. NS1はこれらのIPフラグメントを再構成して27000バイトのSIP応答を形成します。NS1はこの応答を処理します。
5. NS1は応答データをIPフラグメントでCL1に送信します。各IPフラグメントのサイズは、NS1がこれらのフラグメントをCL1に送信するインターフェイス10/1のMTU（9000）以下です。IPフラグメントはLBVS-1のIPアドレスを送信元としています。これらのIPパケットはLBVS-1のIPアドレスを送信元とし、CL1のIPアドレスを宛先としています。

- 最初のIPフラグメントのサイズ === 9000
- 2番目と3番目のIPフラグメントのサイズ === 9000

最後のIPフラグメントのサイズ === 3088

構成タスク:

SDX Management Serviceで、**Configuration > System > Interfaces** ページに移動します。必要なインターフェイスを選択し、**Edit** をクリックします。MTU値を設定し、**OK** をクリックします。

例:

インターフェイス 10/1 の MTU 値を 9000 に、インターフェイス 10/2 の MTU 値を 9000 に設定します。

NetScaler インスタンスにログオンし、ADC コマンドラインインターフェースを使用して、残りの構成手順を完了します。

次の表に、NetScaler インスタンスで必要な構成を作成するためのタスク、コマンド、および例を示します。

タスク	ADC コマンド構文	例
ジャンボフレームをサポートするために、VLAN を作成し、目的の VLAN の MTU を設定します。	<code>add vlan <id> -mtu <positive_integer>; show vlan <id></code>	<code>add vlan 10 -mtu 9000 ; add vlan 20 -mtu 9000</code>
インターフェースを VLAN にバインドします。	<code>bind vlan <id> -ifnum <interface_name>; show vlan <id></code>	<code>bind vlan 10 -ifnum 10/1 ; bind vlan 20 -ifnum 10/2</code>
SNIP アドレスを追加します。	<code>add ns ip <IPAddress> <netmask> -type SNIP ; show ns ip</code>	<code>add ns ip 198.51.100.18 255.255.255.0 -type SNIP</code>
SIPサーバーを表すサービスを作成します。	<code>add service <serviceName> <ip> SIP_UDP <port>; show service <name></code>	サービスを追加 SVC-S1 198.51.100.19 SIP_UDP 5060; サービスを追加 SVC-S2 198.51.100.20 SIP_UDP 5060
SIPロードバランシング仮想サーバーを作成し、サービスをそれにバインドします。	<code>add lb vserver <name> SIP_UDP <ip> <port>; bind lb vserver <vserverName> <serviceName>; show lb vserver <name></code>	<code>add lb vserver LBVS-1 SIP_UDP 203.0.113.15 5060 ; bind lb vserver LBVS-1 SVC-S1 ; bind lb vserver LBVS-1 SVC-S2</code>
<code>bind lb vserver LBVS-1 SVC-S2</code>	<code>save ns config ; show ns config</code>	

ユースケース: 非ジャンボからジャンボへのセットアップ

NetScalerインスタンスNS1で構成されたロードバランシング仮想サーバーLBVS1が、サーバーS1とS2間でトラフィックをロードバランシングするために使用される、非ジャンボからジャンボへ

のセットアップの例を考えてみましょう。クライアントCL1とNS1間の接続は非ジャンボフレームをサポートし、NS1とサーバー間の接続はジャンボフレームをサポートします。

NS1のインターフェース10/1は、クライアントCL1からのトラフィックを受信または送信します。NS1のインターフェース10/2は、サーバーS1またはS2からのトラフィックを受信または送信します。

NS1のインターフェース10/1と10/2は、それぞれVLAN 10とVLAN 20の一部です。CL1とNS1間で非ジャンボフレームのみをサポートするために、インターフェース10/1とVLAN 10の両方でMTUはデフォルト値の1500に設定されています。

NS1とサーバー間でジャンボフレームをサポートするために、インターフェース10/2とVLAN 20のMTUは9000に設定されています。

NS1とサーバー間のサーバーおよびその他すべてのネットワークデバイスも、ジャンボフレームをサポートするように構成されています。HTTPトラフィックはTCPに基づいているため、ジャンボフレームをサポートするために、各エンドポイントでMSSが適切に設定されています。

- CL1とNS1の仮想サーバーLBVS1間の接続では、NS1上のMSSはTCPプロファイルで設定され、そのプロファイルはLBVS1にバインドされます。
- NS1のSNIPアドレスとS1間の接続の場合、NS1上のMSSはTCPプロファイルで設定され、そのプロファイルはNS1上のS1を表すサービス（SVC-S1）にバインドされます。



次の表に、この例で使用されている設定を示します。

エンティティ	名前	詳細
クライアントCL1のIPアドレス	CL1	192.0.2.10
サーバーのIPアドレス	S1	198.51.100.19
	S2	198.51.100.20
インターフェース10/1のMTU （管理サービスインターフェースを使用）。	1500	
インターフェース10/2に設定されたMTU（管理サービスインターフェースを使用）。	9000	

エンティティ	名前	詳細
NS1上のVLAN 10のMTU (ADCコマンドラインインターフェースを使用) .	1500	
NS1上のVLAN 20に設定されたMTU (ADCコマンドラインインターフェースを使用) .	9000	
サーバーを表すNS1上のサービス	SVC-S1	IPアドレス: 198.51.100.19; プロトコル: HTTP; ポート: 80; MSS: 8960
	SVC-S2	IPアドレス: 198.51.100.20; プロトコル: HTTP; ポート: 80; MSS: 8960
VLAN 10上のロードバランシング仮想サーバー	LBVS-1	IPアドレス: 203.0.113.15; プロトコル: HTTP; ポート: 80。バインドされたサービス: SVC-S1, SVC-S2; MSS: 1460

この例における、CL1からS1へのリクエストのトラフィックフローは次のとおりです。

1. クライアントCL1は、NS1の仮想サーバーLBVS-1に送信するために、200バイトのHTTPリクエストを作成します。
2. CL1はNS1のLBVS-1への接続を開きます。CL1とNS1は、接続確立中にそれぞれのTCP MSS値を交換します。
3. NS1のMSSはHTTPリクエストよりも大きいため、CL1はリクエストデータを単一のIPパケットでNS1に送信します。 1.

```
<div id="concept_57AEA1C9D3DA47948B6D834341388D29__d978e142">
```

```
Size of the request packet = [IP Header + TCP Header + TCP Request] =  
[20 + 20 + 200] = 240
```

</div>

4. NS1はインターフェース10/1でリクエストパケットを受信し、そのパケット内のHTTPリクエストデータを処理します。
5. LBVS-1のロードバランシングアルゴリズムはサーバーS1を選択し、NS1はそのSNIPアドレスの1つとS1の間に接続を開きます。NS1とCL1は、接続確立中にそれぞれのTCP MSS値を交換します。
6. S1のMSSはHTTPリクエストよりも大きいため、NS1はリクエストデータを単一のIPパケットでS1に送信します。
 - a. リクエストパケットのサイズ = [IPヘッダー + TCPヘッダー +] = 240

この例における、S1からCL1への応答のトラフィックフローは次のとおりです。

1. サーバーS1は、NS1のSNIPアドレスに送信するために、18000バイトのHTTP応答を作成します。
2. S1は応答データをNS1のMSSの倍数にセグメント化し、これらのセグメントをIPパケットでNS1に送信します。これらのIPパケットはS1のIPアドレスから発信され、NS1のSNIPアドレス宛てです。
 - 最初の2つのパケットのサイズ = = = 9000
 - 最後のパケットのサイズ = = = 2120
3. NS1はインターフェース10/2で応答パケットを受信します。
4. これらのIPパケットから、NS1はすべてのTCPセグメントを組み立てて18000バイトのHTTP応答データを形成します。NS1はこの応答を処理します。
5. NS1は応答データをCL1のMSSの倍数にセグメント化し、これらのセグメントをIPパケットとしてインターフェース10/1からCL1に送信します。これらのIPパケットはLBVS-1のIPアドレスから発信され、CL1のIPアドレス宛てです。
 - 最後のパケットを除くすべてのパケットのサイズ = = = 1500
 - 最後のパケットのサイズ = = = 520

構成タスク:

SDX管理サービスで、**Configuration > System > Interfaces**ページに移動します。必要なインターフェースを選択し、**Edit**をクリックします。MTU値を設定し、**OK**をクリックします。

例:

次のMTU値を設定します。

- 10/1インターフェースの場合、1500
- 10/2インターフェースの場合、9000

NetScalerインスタンスにログオンし、ADCコマンドラインインターフェースを使用して残りの構成手順を完了します。

次の表に、NetScalerインスタンスで必要な構成を作成するためのタスク、コマンド、および例を示します。

タスク	ADCコマンドライン構文	例
VLANを作成し、ジャンボフレームをサポートするために必要なVLANのMTUを設定します。	<pre>add vlan <id> -mtu <positive_integer>; show vlan <id></pre>	<pre>add vlan 10 -mtu 1500; add vlan 20 -mtu 9000</pre>
インターフェースをVLANにバインドします。	<pre>bind vlan <id> -ifnum <interface_name>; show vlan <id></pre>	<pre>bind vlan 10 -ifnum 10/1; bind vlan 20 -ifnum 10/2</pre>
SNIPアドレスを追加します。	<pre>add ns ip <IPAddress> <netmask> -type SNIP; show ns ip</pre>	<pre>add ns ip 198.51.100.18 255.255.255.0 -type SNIP</pre>
HTTPサーバーを表すサービスを作成します	<pre>add service <serviceName> <ip> HTTP <port>; show service <name></pre>	<pre>add service SVC-S1 198.51.100.19 http 80; add service SVC-S2 198.51.100.20 http 80</pre>
HTTP負荷分散仮想サーバーを作成し、サービスをそれにバインドします	<pre>add lb vserver <name> HTTP <ip> <port>; bind lb vserver <vserverName> <serviceName>; show lb vserver <name></pre>	<pre>add lb vserver LBVS-1 http 203.0.113.15 80; bind lb vserver LBVS-1 SVC-S1</pre>
カスタムTCPプロファイルを作成し、ジャンボフレームをサポートするようにMSSを設定します。	<pre>add tcpProfile <name> -mss <positive_integer>; show tcpProfile <name></pre>	<pre>add tcpprofile NS1- SERVERS-JUMBO -mss 8960</pre>

タスク	ADCコマンドライン構文	例
カスタムTCPプロファイルを目的のサービスにバインドします。	<pre>set service <Name> -tcpProfileName <string>; show service <name></pre>	<pre>set service SVC-S1 -tcpProfileName NS1- SERVERS-JUMBO; set service SVC-S2 -tcpProfileName NS1- SERVERS-JUMBO</pre>
設定を保存します	<pre>save ns config; show ns config</pre>	

ユースケース: 同じインターフェースセット上でのジャンボフローと非ジャンボフローの共存

NetScalerインスタンスNS1にロードバランシング仮想サーバーLBVS1とLBVS2が設定されている例を考えてみましょう。LBVS1はサーバーS1とS2間のHTTPトラフィックをロードバランシングするために使用され、グローバルはサーバーS3とS4間のトラフィックをロードバランシングするために使用されます。

CL1はVLAN 10上にあり、S1とS2はVLAN20上にあり、CL2はVLAN 30上にあり、S3とS4はVLAN 40上にあります。VLAN 10とVLAN 20はジャンボフレームをサポートし、VLAN 30とVLAN 40は非ジャンボフレームのみをサポートします。

言い換えれば、CL1とNS1間の接続、およびNS1とサーバーS1またはS2間の接続はジャンボフレームをサポートします。CL2とNS1間の接続、およびNS1とサーバーS3またはS4間の接続は非ジャンボフレームのみをサポートします。

NS1のインターフェース10/1は、クライアントからのトラフィックまたはクライアントへのトラフィックを受信または送信します。NS1のインターフェース10/2は、サーバーからのトラフィックまたはサーバーへのトラフィックを受信または送信します。

インターフェース10/1は、タグ付きインターフェースとしてVLAN 10とVLAN 20の両方にバインドされています。インターフェース10/2は、タグ付きインターフェースとしてVLAN 30とVLAN 40の両方にバインドされています。

ジャンボフレームをサポートするために、インターフェース10/1と10/2のMTUは9216に設定されています。

NS1では、ジャンボフレームをサポートするためにVLAN 10とVLAN 30のMTUが9000に設定されています。非ジャンボフレームのみをサポートするために、VLAN 20とVLAN 40のMTUはデフォルト値の1500に設定されています。

VLANタグ付きパケットのADCインターフェースにおける実効MTUは、インターフェースのMTUまたはVLANのMTUのいずれか低い方です。例：

- インターフェース10/1のMTUは9216です。VLAN 10のMTUは9000です。インターフェース10/1では、VLAN 10タグ付きパケットのMTUは9000です。
- インターフェース10/2のMTUは9216です。VLAN 20のMTUは9000です。インターフェース10/2では、VLAN 20タグ付きパケットのMTUは9000です。
- インターフェース10/1のMTUは9216です。VLAN 30のMTUは1500です。インターフェース10/1では、VLAN 30タグ付きパケットのMTUは1500です。
- インターフェース10/2のMTUは9216です。VLAN 40のMTUは1500です。インターフェース10/2では、VLAN 40タグ付きパケットのMTUは9000です。

CL1、S1、S2、およびCL1とS1またはS2間のすべてのネットワークデバイスは、ジャンボフレーム用に構成されています。

HTTPトラフィックはTCPに基づいているため、ジャンボフレームをサポートするために、各エンドポイントでMSSが適切に設定されます。

- CL1とNS1の仮想サーバーLBVS-1間の接続では、NS1上のMSSはTCPプロファイルで設定され、そのプロファイルはLBVS1にバインドされます。
- NS1のSNIPアドレスとS1間の接続では、NS1上のMSSはTCPプロファイルで設定され、そのプロファイルはNS1上のS1を表すサービス（SVC-S1）にバインドされます。

ジャンボ-非ジャンボ(/en-us/sdx/media/coexist_jumbo_nonjumbo.png)

次の表に、この例で使用されている設定を示します。

エンティティ	名前	詳細
クライアントのIPアドレス	CL1	192.0.2.10
	CL2	192.0.2.20
サーバーのIPアドレス	S1	198.51.100.19
	S2	198.51.100.20

エンティティ	名前	詳細
	S3	198.51.101.19
	S4	198.51.101.20
NS1上のSNIPアドレス	198.51.100.18; 198.51.101.18	
NS1上のインターフェースと VLANに指定されたMTU	10/1	9216
	10/2	9216
VLAN 10	9000	
VLAN 20	9000	
VLAN 30	9000	
VLAN 40	1500	
デフォルトTCPプロファイル	nstcp_default_profile	MSS: 1460
カスタムTCPプロファイル	ALL-JUMBO	MSS: 8960
NS1上のサーバーを表すサー ビス	SVC-S1	IPアドレス: 198.51.100.19; プロトコル: HTTP; ポート: 80; TCPプロファイル: ALL- JUMBO (MSS: 8960)
	SVC-S2	IPアドレス: 198.51.100.20; プロトコル: HTTP; ポート: 80; TCPプロファイル: ALL- JUMBO (MSS: 8960)
	SVC-S3	IPアドレス: 198.51.101.19; プロトコル: HTTP; ポート: 80; TCPプロファイル: nstcp_default_profile (MSS: 1460)
	SVC-S4	IPアドレス: 198.51.101.20; プロトコル: HTTP; ポート:

エンティティ	名前	詳細
		80; TCPプロファイル: nstcp_default_profile (MSS: 1460)
NS1上の負荷分散仮想サーバー	LBVS-1	IPアドレス = 203.0.113.15; プロトコル: HTTP; ポート: 80. バインドされたサービス: SVC-S1, SVC-S2; TCPプロ ファイル: ALL-JUMBO (MSS: 8960)
	LBVS-2	IPアドレス = 203.0.114.15; プロトコル: HTTP; ポート: 80. バインドされたサービス: SVC-S3, SVC-S4; TCPプロ ファイル: nstcp_default_profile (MSS: 1460)

CL1からS1へのリクエストのトラフィックフローは次のとおりです。

1. クライアントCL1は、NS1の仮想サーバーLBVS-1に送信するために、20000バイトのHTTPリクエストを作成します。
2. CL1はNS1のLBVS-1への接続を開きます。接続確立中に、CL1とNS1はそれぞれのTCP MSS値を交換します。
3. NS1のMSS値がHTTPリクエストよりも小さいため、CL1はリクエストデータをNS1のMSSの倍数にセグメント化し、これらのセグメントをVLAN 10としてタグ付けされたIPパケットでNS1に送信します。
 - 最初の2つのパケットのサイズ === 9000
 - 最後のパケットのサイズ === 2120
4. NS1はインターフェース10/1でこれらのパケットを受信します。これらのパケットのサイズが、VLAN 10タグ付きパケットに対するインターフェース10/1の実効MTU（9000）以下であるため、NS1はこれらのパケットを受け入れます。
5. IPパケットから、NS1はすべてのTCPセグメントを組み立てて20000バイトのHTTPリクエストを形成します。NS1はこのリクエストを処理します。

6. LBVS-1の負荷分散アルゴリズムはサーバーS1を選択し、NS1は自身のSNIPアドレスの1つとS1との間に接続を開きます。接続確立中に、NS1とCL1はそれぞれのTCP MSS値を交換します。
7. NS1はリクエストデータをS1のMSSの倍数にセグメント化し、これらのセグメントをVLAN 20としてタグ付けされたIPパケットでS1に送信します。
 - 最初の2つのパケットのサイズ === 9000
 - 最後のパケットのサイズ === 2120

CL1に対するS1の応答のトラフィックフローは次のとおりです。

1. サーバーS1は、NS1のSNIPアドレスに送信するために、30000バイトのHTTP応答を作成します。
2. S1は応答データをNS1のMSSの倍数にセグメント化し、これらのセグメントをVLAN 20としてタグ付けされたIPパケットでNS1に送信します。これらのIPパケットはS1のIPアドレスから発信され、NS1のSNIPアドレス宛てです。
 - 最初の3つのパケットのサイズ === 9000
 - 最後のパケットのサイズ === 3160
3. NS1はインターフェイス10/2で応答パケットを受信します。NS1はこれらのパケットを受け入れます。これは、VLAN 20タグ付きパケットの場合、そのサイズがインターフェイス10/2の有効なMTU値（9000）以下であるためです。
4. これらのIPパケットから、NS1はすべてのTCPセグメントを組み立てて30000バイトのHTTP応答を形成します。NS1はこの応答を処理します。
5. NS1は応答データをCL1のMSSの倍数にセグメント化し、これらのセグメントをVLAN 10としてタグ付けされたIPパケットで、インターフェイス10/1からCL1に送信します。これらのIPパケットはLBVSのIPアドレスから発信され、CL1のIPアドレス宛てです。
 - 最初の3つのパケットのサイズ = [IPヘッダー + TCPヘッダー +] = 9000
 - 最後のパケットのサイズ === 3160

構成タスク:

SDX管理サービスで、**Configuration > System > Interfaces** ページに移動します。必要なインターフェイスを選択し、**Edit** をクリックします。MTU値を設定し、**OK** をクリックします。

例:

次のMTU値を設定します。

- 10/1インターフェイスの場合、9216
- 10/2インターフェイスの場合、9216として

NetScalerインスタンスにログオンし、ADCコマンドラインインターフェースを使用して、残りの設定手順を完了します。

次の表に、NetScalerインスタンスで必要な構成を作成するためのタスク、コマンド、および例を示します。

タスク	構文	例
VLANを作成し、ジャンボフレームをサポートするために、目的のVLANのMTUを設定します。	<pre>add vlan <id> -mtu <positive_integer> ; show vlan <id></pre>	<pre>add vlan 10 -mtu 9000 ; add vlan 20 -mtu 9000 ; add vlan 30 -mtu 1500 ; add vlan 40 -mtu 1500</pre>
インターフェイスをVLANにバインドします。	<pre>bind vlan <id> -ifnum <interface_name> ; show vlan <id></pre>	<pre>bind vlan 10 -ifnum 10/1 -tagged ; bind vlan 20 -ifnum 10/2 -tagged ; bind vlan 30 -ifnum 10/1 -tagged ; bind vlan 40 -ifnum 10/2 -tagged</pre>
SNIPアドレスを追加します。	<pre>add ns ip <IPAddress> <netmask> -type SNIP ; show ns ip</pre>	<pre>add ns ip 198.51.100.18 255.255.255.0 -type SNIP ; a dd ns ip 198.51.101.18 255.255.255.0 -type SNIP</pre>
HTTPサーバーを表すサービスを作成します。	<pre>add service <serviceName> <ip> HTTP <port> ; show service <name></pre>	<pre>add service SVC-S1 198.51.100.19 http 80 ; add service SVC-S2 198.51.100.20 http 80 ; add service SVC-S3 198.51.101.19 http 80 ; add service SVC-S4 198.51.101.20 http 80</pre>
HTTP負荷分散仮想サーバーを作成し、サービスをそれにバインドします。	<pre>add lb vserver <name> HTTP <ip> <port> ; bind lb vserver <vserverName></pre>	<pre>add lb vserver LBVS-1 http 203.0.113.15 80 ; bind lb vserver</pre>

タスク	構文	例
	<pre><serviceName> ; show lb vserver <name></pre>	<pre>LBVS-1 SVC-S1 ; bind lb vserver LBVS-1 SVC-S2</pre>
	<pre>add lb vserver LBVS-2 http 203.0.114.15 80 ; bind lb vserver LBVS-2 SVC-S3 ; bind lb vserver LBVS-2 SVC-S4</pre>	
カスタムTCPプロファイルを作成し、ジャンボフレームをサポートするためにそのMSSを設定します。	<pre>add tcpProfile <name> -mss <positive_integer> ; show tcpProfile <name></pre>	<pre>add tcpprofile ALL- JUMBO -mss 8960</pre>
カスタムTCPプロファイルを、目的の負荷分散仮想サーバーとサービスにバインドします。	<pre>set service <Name> -tcpProfileName <string> ; s how service <name></pre>	<pre>set lb vserver LBVS-1 - tcpProfileName ALL-JUMBO ; s et service SVC-S1 - tcpProfileName ALL-JUMBO ; s et service SVC-S2 - tcpProfileName ALL-JUMBO</pre>
設定を保存します。	<pre>save ns config ; show ns config</pre>	

SDXアプライアンスでのSNMPの設定

NetScaler SDXアプライアンスでSNMPエージェントを設定し、トラップと呼ばれる非同期イベントを生成できます。トラップは、SDXアプライアンスで異常な状態が発生するたびに生成されます。トラップはその後、トラップリスナーと呼ばれるリモートデバイスに送信され、SDXアプライアンスの異常な状態を通知します。

SNMPトラップ宛先の設定、MIBファイルのダウンロード、1つ以上のSNMPマネージャーの設定に加えて、NetScaler SDXアプライアンスをSNMPv3クエリ用に設定できます。

次の図は、SNMPが有効化および設定されたSDXアプライアンスを含むネットワークを示しています。図では、各SNMPネットワーク管理アプリケーションがSNMPを使用してSDXアプライアンス上のSNMPエージェントと通信します。

図1. SNMPをサポートするSDXアプライアンス

ネットワーク図(/en-us/sdx/media/snmp_architectute.png)

SDXアプライアンス上のSNMPエージェントは、SNMPv2にのみ準拠するトラップを生成します。サポートされているトラップは、SDX MIBファイルで確認できます。このファイルは、SDXユーザーインターフェイスのダウンロードページからダウンロードできます。

SNMPトラップ宛先を追加するには

1. 設定タブのナビゲーションペインで、**System > SNMP** を展開し、SNMP Trap Destinations をクリックします。
2. SNMP Trap Destinations ペインで、Add をクリックします。
3. Configure SNMP Trap Destination ページで、次のパラメーターの値を指定します。
 - Destination Server—SNMPトラップメッセージを送信するトラップリスナーのIPv4アドレス。
 - Port—トラップリスナーがトラップメッセージをリッスンするUDPポート。トラップリスナーの設定と一致している必要があります。一致しない場合、リスナーはメッセージを破棄します。最小値: 1。デフォルト: 162。
 - Community—トラップメッセージとともに送信されるパスワード（文字列）。これにより、トラップリスナーはメッセージを認証できます。文字、数字、ハイフン (-)、ピリオド (.)、ハッシュ (#)、スペース ()、アットマーク (@)、等号 (=)、コロン (:)、アンダースコア (_) の文字を含めることができます。注: トラップリスナーデバイスで同じコミュニティ文字列を指定してください。指定しない場合、リスナーはメッセージを破棄します。デフォルト: public。
4. Add をクリックし、Close をクリックします。追加したSNMPトラップ宛先がSNMP Traps ペインに表示されます。

SNMPトラップ宛先のパラメータの値を変更するには、ペインで、変更するトラップ宛先を選択し、をクリックします。ダイアログボックスで、パラメータを変更します。

SNMPトラップを削除するには、ペインで、削除するトラップ宛先を選択し、をクリックします。メッセージボックスで、クリックしてSNMPトラップ宛先を削除します。

MIBファイルのダウンロード

SDXアプライアンスの監視を開始する前に、以下のファイルをダウンロードする必要があります。

SDX-MIB-smiv2.mib。 このファイルは、SNMPv2マネージャーとSNMPv2トラップリスナーによって使用されます。

このファイルには、SDX固有のイベントを提供するNetScalerエンタープライズMIBが含まれています。

MIBファイルをダウンロードするには

1. SDXアプライアンスのユーザーインターフェイスのページにログオンします。
2. の下で、をクリックします。MIBブラウザを使用してファイルを開くことができます。

SNMPマネージャーコミュニティの追加

SDXアプライアンスでSNMPマネージャーを構成して、アプライアンスおよびアプライアンスでホストされている管理対象デバイスを照会および監視します。また、SNMPマネージャーに必要なアプライアンス固有の情報を提供する必要があります。IPv4 SNMPマネージャーの場合、マネージャーのIPアドレスの代わりにホスト名を指定できます。その場合、SNMPマネージャーのホスト名をそのIPアドレスに解決するDNSネームサーバーを追加する必要があります。

少なくとも1つのSNMPマネージャーを構成します。SNMPマネージャーを構成しない場合、アプライアンスはネットワーク上のどのIPアドレスからのSNMPクエリも受け入れず、応答しません。1つ以上のSNMPマネージャーを構成した場合、アプライアンスはそれらの特定のIPアドレスからのSNMPクエリのみを受け入れ、応答します。

SNMPマネージャーを構成するには

1. タブのナビゲーションペインで、を展開し、次にを展開します。
2. をクリックします。
3. 詳細ペインで、をクリックします。
4. 「SNMPマネージャーコミュニティの作成」ページで、次のパラメータを設定します。
 - SNMPマネージャー — SNMPマネージャーのIPv4アドレス。または、IPv4アドレスの代わりに、SNMPマネージャーに割り当てられているホスト名を指定することもできます。その場合、SNMPマネージャーのホスト名をIPアドレスに解決するDNSネームサーバーを追加する必要があります。
 - コミュニティ — SNMPコミュニティ文字列。大文字と小文字、数字、ハイフン (-)、ピリオド (.)、シャープ (#)、アットマーク (@)、等号 (=)、コロン (:)、アンダースコア (_) の文字を含む1~31文字で構成できます。
 - ネットマスクを使用してSNMPマネージャーを指定するには、チェックボックスをオンにします。

- フィールドに、SNMPコミュニティのネットマスクを入力します。

5. をクリックし、次に をクリックします。

SNMPv3クエリ用にSDXアプライアンスを構成する

SNMPv3は、SNMPv1およびSNMPv2の基本的な構造とアーキテクチャに基づいています。ただし、SNMPv3は、認証、アクセス制御、データ整合性チェック、データ発信元検証、メッセージ適時性チェック、データ機密性などの管理およびセキュリティ機能を組み込むために、基本的なアーキテクチャを強化しています。

NetScaler SDXアプライアンスは、SNMPv3のセキュリティ機能を実装するために、次のエンティティをサポートしています。

- SNMPビュー
- SNMPユーザー

これらのエンティティは連携してSNMPv3セキュリティ機能を実装します。ビューは、MIBのサブツリーへのアクセスを許可するために作成されます。

SNMPマネージャーの追加

適切なSNMPマネージャーがSDXアプライアンスにクエリを実行できるように構成します。また、SNMPマネージャーに必要なアプライアンス固有の情報を提供します。IPv4 SNMPマネージャーの場合、マネージャーのIPアドレスの代わりにホスト名を指定できます。その場合、SNMPマネージャーのホスト名をIPアドレスに解決するDNSネームサーバーを追加する必要があります。

少なくとも1つのSNMPマネージャーを構成します。SNMPマネージャーを構成しない場合、アプライアンスはネットワーク上のどのIPアドレスからのSNMPクエリも受け入れず、応答しません。1つ以上のSNMPマネージャーを構成した場合、アプライアンスはそれらの特定のIPアドレスからのSNMPクエリのみを受け入れ、応答します。

SNMPマネージャーを構成するには：

1. **System > Configuration** ページに移動します。
2. Configurationタブのナビゲーションペインで、Systemを展開し、次にSNMPを展開します。
3. Managersをクリックします。
4. 詳細ペインで、Addをクリックします。
5. Add SNMP Manager Communityダイアログボックスで、次のパラメータを設定します。

- **SNMPマネージャー**—SNMPマネージャーのIPv4アドレス。または、IPv4アドレスの代わりに、SNMPマネージャーに割り当てられているホスト名を指定できます。その場合、SNMPマネージャーのホスト名をそのIPアドレスに解決するDNSネームサーバーを追加する必要があります。
- **コミュニティ**—SNMPコミュニティ文字列。大文字と小文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、アットマーク (@)、等号 (=)、コロン (:)、アンダースコア () の文字を含む1~31文字で構成できます。

6. Addをクリックし、次にCloseをクリックします。

SNMPビューの構成

SNMPビューは、MIBの特定のセクションへのユーザーアクセスを制限します。SNMPビューはアクセス制御の実装に使用されます。

ビューを構成するには

1. Configurationタブのナビゲーションペインで、Systemを展開し、次にSNMPを展開します。
2. Viewsをクリックします。
3. 詳細ペインで、をクリックします。
4. SNMPビューの追加ダイアログボックスで、次のパラメータを設定します。
 - **名前** — SNMPv3ビューの名前。大文字と小文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、アットマーク (@)、等号 (=)、コロン (:)、アンダースコア () の文字を含む1~31文字で構成できます。SNMPv3ビューを識別しやすい名前を選択してください。
 - **サブツリー** — このSNMPv3ビューに関連付けるMIBツリーの特定のブランチ（サブツリー）。サブツリーをSNMP OIDとして指定します。
 - **タイプ** — サブツリーパラメータで指定されたサブツリーをこのビューに含めるか除外するか。この設定は、SNMPv3ビューにAのようなサブツリーを含めており、そのAの特定のサブツリー（Bなど）をSNMPv3ビューから除外したい場合に役立ちます。

SNMPユーザーの構成

SNMPビューを作成したら、SNMPユーザーを追加します。SNMPユーザーは、SNMPマネージャーのクエリに必要なMIBにアクセスできます。

ユーザーを構成するには

1. 構成タブのナビゲーションペインで、を展開し、次にを展開します。
2. をクリックします。

3. 詳細ペインで、をクリックします。

4. SNMPユーザーの作成ページで、次のパラメータを設定します。

- 名前 — SNMPv3ユーザーの名前。大文字と小文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、アットマーク (@)、等号 (=)、コロン (:)、アンダースコア (_) の文字を含む1~31文字で構成できます。
- セキュリティレベル — アプライアンスとSNMPv3ユーザー間の通信に必要なセキュリティレベル。次のいずれかのオプションから選択します。
 - noAuthNoPriv — 認証も暗号化も不要です。
 - authNoPriv—認証は必要だが、暗号化は不要。
 - authPriv—認証と暗号化の両方が必要。
- 認証プロトコル—アプライアンスとSNMPv3ユーザー間の通信を認証するために使用される認証アルゴリズム。SNMPマネージャーでSNMPv3ユーザーを設定するには、同じ認証アルゴリズムを指定してください。
- 認証パスワード—認証アルゴリズムで使用されるパスフレーズ。大文字と小文字の英字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等号 (=)、コロン (:)、アンダースコア (_) の文字を含む1~31文字で構成できます。
- プライバシープロトコル—アプライアンスとSNMPv3ユーザー間の通信を暗号化するために使用される暗号化アルゴリズム。SNMPマネージャーでSNMPv3ユーザーを設定するには、同じ暗号化アルゴリズムを指定してください。
- ビュー名—このSNMPv3ユーザーにバインドする、設定済みのSNMPv3ビューの名前。SNMPv3ユーザーは、このSNMPv3ビューにINCLUDEDタイプとしてバインドされているサブツリーにはアクセスできますが、EXCLUDEDタイプのものにはアクセスできません。

SNMPアラームの設定

アプライアンスは、SNMPアラームと呼ばれる事前定義された条件エンティティのセットを提供します。SNMPアラームの条件セットが満たされると、アプライアンスは設定されたトラップリスナーに送信されるSNMPトラップメッセージを生成します。たとえば、deviceAddedアラームが有効になっている場合、アプライアンスにデバイス（インスタンス）がプロビジョニングされるたびにトラップメッセージが生成され、トラップリスナーに送信されます。SNMPアラームに重大度レベルを割り当てることができます。そうすると、対応するトラップメッセージにその重大度レベルが割り当てられます。

アプライアンスで定義されている重大度レベルを、重大度の高い順に示します。

- 重大
- 主要
- 軽微
- 警告
- 情報 (デフォルト)

たとえば、deviceAddedという名前のSNMPアラームに警告の重大度レベルを設定した場合、デバイスが追加されたときに生成されるトラップメッセージには警告の重大度レベルが割り当てられます。

アラームの条件が満たされるたびに生成される対応するトラップメッセージをログに記録するように、SNMPアラームを設定することもできます。

定義済みのSNMPアラームを変更するには、**System > SNMP > Alarms**をクリックします。

Management Serviceインベントリの不一致を監視するためのアラーム

Management Serviceは、そのインベントリ内のすべてのインターフェイスとチャンネルを監視し、Management Serviceデータベース、Xenサーバー、およびVPX間の不一致をチェックします。

チャンネルまたはインターフェイスの詳細に不一致が見つかった場合、

「VPXInterfacesNotInSync」アラームをトリガーします。この機能はバージョン14.1-34.x以降で利用可能です。

VPXインターフェイスの同期不一致アラーム(/en-us/sdx/media/vpx-interfaces-arenot-insync-alarm.png)

syslog通知を設定する

SYSLOGは標準のロギングプロトコルです。これには、NetScaler SDXアプライアンスで実行されるSYSLOG監査モジュールと、リモートシステムで実行できるSYSLOGサーバーの2つのコンポーネントがあります。SYSLOGはデータ転送にUDPを使用します。

SYSLOGサーバーを実行すると、SDXアプライアンスに接続されます。その後、アプライアンスはすべてのログ情報をSYSLOGサーバーに送信し始め、サーバーはログエントリをログファイルに保存する前にフィルタリングできます。SYSLOGサーバーは複数のSDXアプライアンスからログ情報を受信でき、SDXアプライアンスは複数のSYSLOGサーバーにログ情報を送信できます。

SYSLOGサーバーがSDXアプライアンスから収集するログ情報は、メッセージの形式でログファイルに保存されます。これらのメッセージには通常、次の情報が含まれます。

- ログメッセージを生成したSDXアプライアンスのIPアドレス
- タイムスタンプ
- メッセージタイプ
- ログレベル（クリティカル、エラー、ノーティス、ワーニング、インフォメーションアル、デバッグ、アラート、またはエマージェンシー）
- メッセージ情報

この情報を使用して、アラートの原因を分析し、必要に応じて是正措置を講じることができます。まず、アプライアンスがログ情報を送信するsyslogサーバーを設定し、次にログメッセージを記録するためのデータと時刻の形式を指定します。

syslogサーバーを設定する

1. **System > Notifications > Syslog Servers** に移動します。
2. 詳細ペインで、**Add** をクリックします。
3. **Create Syslog Server** ページで、syslogサーバーのパラメーターの値を指定します。パラメーターの説明については、対応するフィールドにマウスを合わせます。
4. **Add** をクリックし、次に **Close** をクリックします。

Syslog パラメータを設定する

1. **System > Notifications > Syslog Servers** に移動します。
2. 詳細ペインで、**Syslog Parameters** をクリックします。
3. **Syslog パラメータの構成** ページで、日付と時刻の形式を指定します。
4. **OK** をクリックし、次に **Close** をクリックします。

メール通知の構成

アラートが発生するたびにメールメッセージを受信するようにSMTPサーバーを構成します。まずSMTPサーバーを構成し、次にメールプロファイルを構成します。メールプロファイルでは、受信者のアドレスをコンマで区切って指定します。

SMTPサーバーを構成するには

1. **System > Notifications > Email** に移動します。
2. 詳細ペインで、**Email Server** タブをクリックし、**Add** をクリックします。
3. **Create Email Server** ページで、サーバーパラメータの値を指定します。

- **サーバー名 / IPアドレス:** SMTPメールサーバーのサーバー名またはIPアドレスを入力します。
- **ポート:** ポート番号を入力します。デフォルト値は25です。
- **認証:** メールサーバーへのアクセスを認証するには、このオプションを選択します。
- **セキュア:** セキュアなメール接続を作成するには、このオプションを選択します。デフォルトでは、TLS 1.2がメール通信の暗号化に使用されます。

4. **Create** をクリックします。



メールプロファイルを構成するには

1. **System > Notifications > Email** に移動します。
2. 詳細ペインで、**Email** タブをクリックし、**Add** をクリックします。
3. 「メール配信リストの作成」ページで、パラメータの値を指定します。パラメータの説明については、対応するフィールドにマウスを合わせます。
4. 「作成」をクリックします。

SMS通知を構成する

アラートが生成されるたびにSMSメッセージを受信するように、ショートメッセージサービス (SMS) サーバーを構成します。まずSMSサーバーを構成し、次にSMSプロファイルを構成します。SMSプロファイルでは、受信者のアドレスをコンマで区切ります。

SMSサーバーを構成する

1. **System > Notifications > SMS** に移動します。
2. 詳細ペインで、**SMS Server** をクリックし、次に **Add** をクリックします。
3. **Create SMS Server** ページで、SMSサーバーパラメーターの値を指定します。これらのパラメーターの値は、ベンダーによって提供されます。
4. **Create** をクリックし、次に **Close** をクリックします。

SMSプロファイルを構成する

1. **System > Notifications > SMS** に移動します。
2. 詳細ペインで、**SMS Distribution List** をクリックし、次に **Add** をクリックします。

3. **Create SMS Distribution List** ページで、メールプロファイルパラメーターの値を指定します。パラメーターの説明については、対応するフィールドにマウスを合わせます。
4. **Create** をクリックし、次に **Close** をクリックします。

SDXアプライアンスに構成されたエンティティのリアルタイムステータスを監視および管理する

NetScaler SDXアプライアンスは、SDXアプライアンスでホストされている仮想アプライアンス全体の仮想サーバー、サービス、サービスグループ、およびサーバーの状態を監視および管理できます。仮想サーバーの健全性や、サービスまたはサービスグループの最後の状態変更からの経過時間などの値を監視できます。この監視により、エンティティのリアルタイムステータスが可視化され、NetScalerインスタンスに多数のエンティティが構成されている場合に、これらのエンティティの管理が容易になります。

仮想サーバーのステータスを表示する

仮想サーバーの状態と健全性のリアルタイム値を監視できます。また、仮想サーバーの名前、IPアドレス、仮想サーバーのタイプなどの属性も表示できます。

仮想サーバーのステータスを表示するには

1. 設定タブのナビゲーションペインで、**NetScaler > エンティティ > 仮想サーバー**をクリックします。
2. 右ペインの「仮想サーバー」で、次の統計情報を表示します。
 - デバイス名 – 仮想サーバーが構成されているVPXの名前。
 - 名前 – 仮想サーバーの名前。
 - プロトコル – 仮想サーバーのサービスタイプ。例：HTTP、TCP、SSL。
 - 有効な状態 – バックアップ仮想サーバーの状態に基づいて、仮想サーバーの有効な状態。例：UP、DOWN、またはOUT OF SERVICE。
 - 状態 – 仮想サーバーの現在の状態。例：UP、DOWN、またはOUT OF SERVICE。
 - 健全性 – UP状態であり、仮想サーバーにバインドされているサービスの割合。健全性パーセンテージの計算には、次の式が使用されます。(バインドされたUPサービスの数 * 100) / バインドされたサービスの合計

- IPアドレス — 仮想サーバーのIPアドレス。クライアントはこのIPアドレスに接続要求を送信します。
- ポート — 仮想サーバーがクライアント接続をリッスンするポート。
- 最終状態変更 — 仮想サーバーの状態が最後に変更されてからの経過時間（日、時間、分、秒）。つまり、仮想サーバーが現在の状態であった期間です。この情報は、NetScalerリリース9.0以降で構成された仮想サーバーでのみ利用可能です。

仮想サーバーにバインドされているサービスとサービスグループの表示

仮想サーバーにバインドされているサービスとサービスグループのリアルタイムステータスを監視できます。この監視により、仮想サーバーの健全性パーセンテージが低下する可能性のあるサービスの状態を確認し、適切な措置を講じることができます。

仮想サーバーにバインドされているサービスとサービスグループを表示するには

1. 構成タブの左ペインで、**NetScaler > エンティティ > 仮想サーバー**をクリックします。
2. 詳細ペインの「仮想サーバー」で、バインドされているサービスとサービスグループを表示したい仮想サーバーの名前をクリックし、「アクション」で「バインドされているサービス」または「バインドされているサービスグループ」をクリックします。または、仮想サーバーの名前を右クリックし、「バインドされているサービス」または「バインドされているサービスグループ」をクリックします。

サービスの状態を表示する

サービスの状態のリアルタイム値と、そのサービスが現在の状態であった期間を監視できます。

仮想サーバーの状態を表示するには

1. 構成タブのナビゲーションペインで、**NetScaler > エンティティ > サービス**をクリックします。
2. 詳細ペインの「サービス」で、次の統計情報を表示します。
 - デバイス名 — サービスが構成されているデバイスの名前。

- 名前 — サービスの名前。
- プロトコル — サービスの動作を決定するサービスタイプ。例：HTTP、TCP、UDP、またはSSL。
- 状態 — サービスの現在の状態。例：UP、DOWN、またはOUT OF SERVICE。
- IPアドレス — サービスのIPアドレス。
- ポート — サービスがリスンするポート。
- 最終状態変更 — サービスの最終状態変更からの経過時間（日、時間、分、秒）。つまり、サービスが現在の状態にある期間です。

サービスがバインドされている仮想サーバーの表示

サービスがバインドされている仮想サーバーを表示し、仮想サーバーのリアルタイムステータスを監視できます。

サービスがバインドされている仮想サーバーを表示するには

1. 構成タブのナビゲーションペインで、**NetScaler > エンティティ > サービス**をクリックします。
2. 詳細ペインの[サービス]で、バインドされている仮想サーバーを表示したいサービスの名前をクリックします。次に、[アクション]メニューから[バインドされている仮想サーバー]を選択します。または、サービスを右クリックし、[バインドされている仮想サーバー]をクリックします。

サービスグループのステータスを表示する

SDXインターフェイスからサービスグループメンバーのリアルタイムの状態を監視できます。

サービスグループのステータスを表示するには

1. 構成タブのナビゲーションペインで、**NetScaler > エンティティ > サービスグループ**をクリックします。
2. 詳細ペインので、次の統計情報を表示します。
 - デバイス名 — サービスグループが構成されているデバイスの名前。

- 名前 — サービスグループの名前。
- IPアドレス—サービスグループのメンバーである各サービスのIPアドレス。
- ポート—サービスグループのメンバーがリスンするポート。
- プロトコル—サービスグループの動作を決定するサービスタイプ。例: HTTP、TCP、UDP、またはSSL。
- 有効な状態—バックアップ仮想サーバーの状態に基づいて、仮想サーバーグループの有効な状態。例: UP、DOWN、またはOUT OF SERVICE
- 状態—サービスグループのメンバーの状態に基づいて、サービスグループの有効な状態。例: UP、DOWN、またはOUT OF SERVICE。
- 最終状態変更—サービスグループメンバーの状態が最後に変更されてからの経過時間（日、時間、分、秒）。つまり、サービスグループメンバーが現在の状態であった期間。この情報は、NetScalerリリース9.0以降で構成されたサービスグループメンバーに対してのみ利用可能です。

サービスがバインドされている仮想サーバーの表示

サービスがバインドされている仮想サーバーを表示し、仮想サーバーのリアルタイムステータスを監視できます。

サービスがバインドされている仮想サーバーを表示するには

1. 構成タブの左ペインで、**NetScaler > エンティティ > サーバー**をクリックします。
2. 右ペインの「サーバー」で、リストからサーバーを選択し、「アクション」メニューの「バインドされた仮想サービス」をクリックします。または、サービスを右クリックして「バインドされた仮想サーバー」をクリックします。

サーバーのステータスを表示する

NetScalerインスタンス全体のサーバーの状態を監視および管理できます。この監視により、サーバーのリアルタイムステータスが可視化され、多数のサーバーがある場合でもこれらのサーバーの管理が容易になります。

サーバーのステータスを表示するには

1. 構成タブのナビゲーションペインで、**NetScaler > エンティティ > サーバー**をクリックします。
2. 詳細ペインの で、次の統計を表示します。
 - デバイス名: サーバーが構成されているデバイスの名前を指定します。
 - 名前: サーバーの名前を指定します。
 - IPアドレス: サーバーのIPアドレスを指定します。クライアントはこのIPアドレスに接続要求を送信します。
 - 状態: サーバーの現在の状態を指定します。たとえば、UP、DOWN、OUT OF SERVICEなどです。
 - 最終状態変更: サーバーの状態が最後に変更されてからの経過時間（日、時間、分、秒）を指定します。つまり、サーバーが現在の状態にある期間です。

ポーリング間隔を構成する

SDXアプライアンスが仮想サーバー、サービス、サービスグループ、およびサーバーのリアルタイム値をポーリングする時間間隔を設定できます。デフォルトでは、アプライアンスは30分ごとに値をポーリングします。

仮想サーバー、サービス、サービスグループ、およびサーバーのポーリング間隔を構成するには。

1. 構成タブで、****NetScaler > エンティティ****をクリックし、右側のペインで [ポーリング間隔の構成] をクリックします。
2. [ポーリング間隔の構成] ダイアログボックスで、SDXがエンティティ値をポーリングする時間間隔として設定する分数値を入力します。ポーリング間隔の最小値は30分です。[OK] をクリックします。

NetScalerインスタンスで生成されたイベントの監視と管理

イベント機能を使用して、NetScalerインスタンスで生成されたイベントを監視および管理します。管理サービスはイベントをリアルタイムで識別し、問題に即座に対処するのに役立ち、NetScalerインスタンスを効果的に稼働させ続けます。イベントルールを設定して、生成されたイベントをフィルタリングし、フィルタリングされたイベントリストに対してアクションを実行するように通知を受け取ることもできます。

すべてのイベントを表示する

NetScaler SDXアプライアンスにプロビジョニングされたNetScalerインスタンスで生成されたすべてのイベントを表示できます。各イベントの重大度、カテゴリ、日付、ソース、メッセージなどの詳細を表示できます。

イベントを表示するには、**Configuration > NetScaler > Events > All Events** に移動します。

イベントの表示(/en-us/sdx/media/events-1.png)

イベントを選択し、**Details** ボタンをクリックすると、イベント履歴とエンティティの詳細を表示できます。このページから特定のイベントを検索したり、削除したりすることもできます。

注: イベントを削除すると、復元することはできません。

- レポートの表示

レポートページには、イベントの概要がグラフィカルな形式で表示されます。レポートの表示は、さまざまな時間スケールに基づいて行うことができます。デフォルトでは、時間スケールは「日」です。

レポートを表示するには、**Configuration > NetScaler > Events > Reports** に移動します。以下は、管理サービスでサポートされているグラフィカルレポートです。

- イベント

イベントレポートは、イベント数を円グラフで表示したもので、重大度に基づいてセグメント化され、色分けされています。

イベント円グラフ(/en-us/sdx/media/events-2.png)

特定の重大度のイベントの詳細を表示するには、円グラフのそのセグメントをクリックすると、以下の詳細を表示できます。

- ソース: イベントが生成されたシステム名、ホスト名、またはIPアドレス。
- 日付: アラームが生成された日時。
- カテゴリ: イベントカテゴリ (例: `entityup`)。
- メッセージ: イベントの説明。

- すべてのイベント別NetScalerインスタンス上位10

このレポートは、選択した時間スケールでのイベント数に基づいて、上位10のNetScalerインスタンスを表示する棒グラフです。



◦ **エンティティ状態変更イベント別NetScalerインスタンス上位10**

このレポートは、選択した時間スケールでのエンティティ状態変更の数に基づいて、上位10のNetScalerインスタンスを表示する棒グラフです。エンティティの状態変更は、エンティティアップ、エンティティダウン、またはサービス停止イベントを反映します。



◦ **しきい値違反イベント別NetScalerインスタンス上位10**

このレポートは、選択した時間スケールでのしきい値違反イベントの数に基づいて、上位10のNetScalerインスタンスを表示する棒グラフです。しきい値違反イベントは、次のイベントを反映します:

- cpuUtilization
 - memoryUtilization
 - diskUsageHigh
 - 温度高
 - 電圧低
 - 電圧高
 - ファン速度低
 - CPU温度高
 - インターフェーススループット低
 - インターフェース帯域幅使用率高
 - 集約帯域幅使用率高
- **ハードウェア障害イベントによるNetScalerインスタンス上位10件** このレポートは、選択した時間スケールにおけるハードウェア障害イベントの数に基づいて、NetScalerインスタンスの上位10件を表示する棒グラフです。ハードウェア障害イベントには、以下のイベントが含まれます。
- ハードディスクドライブエラー
 - コンパクトフラッシュエラー
 - 電源障害
 - "SSLカード障害"
- **構成変更イベントによるNetScalerインスタンス上位10件**

このレポートは、選択した時間スケールにおける構成変更イベントの数に基づいて、NetScalerインスタンスの上位10件を反映する棒グラフです。グラフをクリックすると、インスタンスのユーザーベースの構成変更をドリルダウンして表示できます。このグラフをクリックすると、承認および実行ステータスの詳細をさらに表示できます。

。 認証失敗イベントによるNetScalerインスタンス上位10件

このレポートは、選択した時間スケールにおける認証失敗イベントの数に基づいて、上位10件のNetScalerインスタンスを表示する棒グラフです。グラフをクリックすると、ドリルダウンしてインスタンスごとのユーザーベースの認証失敗を表示できます。



。 イベントルールの構成

特定の条件を持つルールを構成し、そのルールにアクションを割り当てることで、一連のイベントをフィルタリングできます。生成されたイベントがルールのフィルタ条件を満たすと、ルールに関連付けられたアクションが実行されます。フィルタを作成できる条件は、重大度、デバイス、失敗オブジェクト、カテゴリです。

イベントには次のアクションを割り当てることができます。

- 。 **電子メール送信アクション** フィルタ条件に一致するイベントに対して電子メールを送信します。
- 。 **SMS送信アクション** フィルタ条件に一致するイベントに対してショートメッセージサービス (SMS) を送信します。

イベントルールを追加するには

a. **Configuration > NetScaler > Events > Event Rules** に移動し、 をクリックします。

b. ルールページで、次のパラメータを設定します。

- 。 名前—イベントルールの名前。
- 。 有効—イベントルールを有効にします。
- 。 重大度—イベントルールを追加するイベントの重大度。
- 。 デバイス—イベントルールを定義するNetScalerインスタンスのIPアドレス。
- 。 カテゴリ — NetScalerインスタンスによって生成されたイベントのカテゴリまたは複数のカテゴリ。
- 。 障害オブジェクト — イベントが生成されたエンティティインスタンスまたはカウンタ。



注: このリストには、すべてのしきい値関連イベントのカウンタ名、すべてのエンティティ関連イベントのエンティティ名、および証明書関連イベントの証明書名を含めることができます。

c. 「保存」をクリックします。

d. 「ルールアクション」で、イベントの通知アクションを割り当てることができます。

a. メールプロファイル — メールサーバーとメールプロファイルの詳細。イベントが定義されたフィルタ条件を満たすと、メールがトリガーされます。

b. SMSプロファイル — SMSサーバーとSMSプロファイルの詳細。イベントが定義されたフィルタ条件を満たすと、SMSがトリガーされます。



e. 「完了」をクリックします。

• イベントの構成

SDXアプライアンス上のNetScalerインスタンスに対して生成されるイベントに、重大度レベルを割り当てることができます。次の種類の重大度レベルを定義できます: 重大、メジャー、マイナー、警告、クリア、情報。特定の時間、イベントを抑制することもできます。重大度を構成するには:

a. **構成 > NetScaler > イベント > イベント構成**に移動し、リストからイベントを選択して、「重大度の構成」をクリックします。



b. 「イベント構成の構成」ページで、ドロップダウンリストから必要な重大度レベルを選択します。

c. または、チェックボックスをオンにすることで、イベントを抑制できます。また、オプションを使用して、このイベントを抑制したいNetScalerインスタンスを指定することもできます。



d. をクリックします。

イベントを削除する

リリース14.1ビルド25.x以降、NetScalerインスタンス用に生成されたイベントを削除できます。

1. **構成 > NetScaler > イベント > すべてのイベント** に移動します。

2. 1つ以上のイベントを選択し、**削除** をクリックします。
3. **確認** ページで、**はい** をクリックして生成されたイベントを削除します。



SDXアプライアンス上のNetScalerインスタンスに対するCall Homeサポート

Call Home機能は、NetScalerインスタンスの一般的なエラー状態を監視します。Management Serviceユーザーインターフェイスから、NetScalerインスタンスのCall Home機能を構成、有効化、または無効化できるようになりました。

注： アプライアンスで事前定義されたエラー状態が発生した場合にCall Homeがシステムデータをサーバーにアップロードできるようにするには、NetScalerインスタンスがCitrixテクニカルサポートサーバーに登録されている必要があります。NetScalerインスタンスでCall Home機能を有効にすると、登録プロセスが開始されます。

NetScalerインスタンスでのCall Homeの有効化と無効化

Management ServiceからNetScalerインスタンスでCall Home機能を有効にできます。Call Home機能を有効にすると、Call HomeプロセスはNetScalerインスタンスをCitrixテクニカルサポートサーバーに登録します。登録には時間がかかります。その間、Management Serviceは登録の進行状況を表示します。

Call Home機能を有効にするには、**Configuration > NetScaler > Call Home** に移動し、NetScalerインスタンスを選択して、Enableボタンをクリックします。確認ページで、Yesをクリックします。

Call Home機能を無効にするには、**Configuration > NetScaler > Call Home** に移動し、NetScalerインスタンスを選択して、Disableボタンをクリックします。確認ページで、Yesをクリックします。

Call Homeを有効にすると、次のオプションを構成できます。

1. (オプション) 管理者のメールアドレスを指定します。Call Homeプロセスは、このメールアドレスをサポートサーバーに送信し、Call Homeに関する今後の連絡のために保存されます。
2. (オプション) Call Homeプロキシモードを有効にします。Call Homeは、プロキシサーバーを介してNetScalerインスタンスのデータをCitrix TaaSサーバーにアップロードできます。この機能を使用するには、NetScalerインスタンスでこれを有効にし、HTTPプロキシサーバーのIPアドレスとポート番号を指定します。プロキシサーバーからTaaSサーバー（インターネット経由）へのすべてのトラフィックはSSL経由で暗号化されるため、データセキュリティとプライバシーが損なわれることはありません。

Management ServiceからNetScalerインスタンスでCall Homeを構成するには

Call Home機能は、単一のインスタンスまたは複数のインスタンスで同時に構成できます。

単一のNetScalerインスタンスでCall Home機能を構成するには、****Configuration > NetScaler > Call Home**** に移動し、NetScalerインスタンスを選択して、Configureボタンをクリックします。Configure Call Homeページで、OKをクリックします。

! [コールホーム設定1] (<https://docs.netScaler.com/content/dam/netScaler/us/en/sdx/media/call-home-1.png>)

複数のNetScalerインスタンスでCall Home機能を構成するには、****Configuration > NetScaler**** に移動します。右ペインでCall Homeをクリックします。Configure Call Homeページで、Available InstancesセクションからNetScalerインスタンスを選択し、その他の詳細を指定して、OKをクリックします。

! [コールホーム設定2] (<https://docs.netScaler.com/content/dam/netScaler/us/en/sdx/media/call-home-2.png>)

-

NetScalerインスタンスのポーリング

すべてのNetScalerインスタンスからCall Home機能をポーリングし、現在のステータスを表示するには、**Configuration > NetScaler > Call Home** に移動し、**Poll Now** をクリックします。確認ページで、**Yes** をクリックします。

システムヘルス監視

システムヘルス監視は、監視対象コンポーネントのエラーを検出し、障害を回避するための是正措置を講じることができます。NetScaler SDXアプライアンスでは、以下のコンポーネントが監視されます。

- ハードウェアおよびソフトウェアリソース
- 物理ディスクと仮想ディスク
- ファン、温度、電圧、電源センサーなどのハードウェアセンサー
- インターフェイス

タブで、 をクリックします。すべてのコンポーネントの概要が表示されます。監視対象コンポーネントの詳細を表示するには、 を展開し、監視するコンポーネントをクリックします。

- SDXアプライアンスのリソースの監視

SDXアプライアンスのハードウェアおよびソフトウェアコンポーネントを監視し、必要に応じて是正措置を講じることができます。監視対象コンポーネントを表示するには、 タブで を展開し、 をクリックします。ハードウェアおよびソフトウェアリソースの詳細が表示されます。すべてのハードウェアコンポーネントについて、現在値と期待値が表示されます。ソフトウェアコンポーネントについては、BMCファームウェアバージョンを除き、現在値と期待値は「該当なし (NA)」と表示されます。

- **名前:** CPU、メモリ、BMCファームウェアバージョンなど、コンポーネントの名前。
- **ステータス:** コンポーネントの状態（条件）です。ハードウェアおよびBMCファームウェアバージョンでは、ERRORは期待値からの逸脱を示します。Citrix Hypervisor™への呼び出しの場合、ERRORは、管理サービスがAPI、HTTP、PING、またはSSH呼び出しを使用してCitrix Hypervisorと通信できないことを示します。ヘルスマニタープラグインの場合、ERRORは、プラグインがCitrix Hypervisorにインストールされていないことを示します。
- **現在値:** コンポーネントの現在値。通常の状態では、現在値は期待値と同じです。
- **期待値:** コンポーネントの期待値。Citrix Hypervisorへのソフトウェア呼び出しには適用されません。

SDXアプライアンスのストレージリソースを監視する

SDXアプライアンスのディスクを監視し、必要に応じて是正措置を講じることができます。監視対象コンポーネントを表示するには、タブで を展開し、 をクリックします。物理ディスク、および物理ディスクから作成された仮想ディスクまたはパーティションの詳細が表示されます。

ディスク (Disk) の場合、以下の詳細が表示されます。

- **名前:** 物理ディスクの名前。
- **サイズ:** ディスクのサイズ (GB単位)。
- **使用済み:** ディスク上のデータ量 (GB単位)。
- **トランザクション/秒:** 1秒あたりに読み書きされるブロック数。この数値は `iostat` 出力から読み取られます。
- **読み取りブロック/秒:** 1秒あたりに読み取られるブロック数。この値を使用して、ディスクからの出力レートを測定できます。
- **書き込みブロック/秒:** 1秒あたりに書き込まれるブロック数。この値を使用して、ディスクへの入力レートを測定できます。
- **総読み取りブロック数:** アプライアンスが最後に起動されてから読み取られたブロックの総数。
- **総書き込みブロック数:** アプライアンスが最後に起動されてから書き込まれたブロックの総数。

仮想ディスクまたはパーティション (Storage Repository) の場合、以下の詳細が表示されます。

- **ドライブベイ:** ドライブベイ内のドライブの番号。このパラメータでデータをソートできます。
- **ステータス:** ドライブベイ内のドライブの状態。可能な値:
 - GOOD: ドライブは良好な状態であり、使用準備ができています。
 - FAIL: ドライブが故障しており、交換する必要があります。
 - MISSING: ドライブベイでドライブが検出されません。
 - 不明: ドライブベイに新しい未フォーマットのドライブが存在します。
- **名前:** ストレージリポジトリのシステム定義名。
- **サイズ:** ストレージリポジトリのサイズ (GB単位)。
- **使用済み:** ストレージリポジトリ内のデータ量 (GB単位)。

SDXアプライアンスのハードウェアセンサーを監視する

SDXアプライアンスのハードウェアコンポーネントを監視し、必要に応じて是正措置を講じることができます。監視タブで、システムヘルスを展開し、ハードウェアセンサーをクリックします。監視機能は、さまざまなファンの速度、さまざまなコンポーネントの温度と電圧、および電源の状態に関する詳細を表示します。

ファン速度については、次の詳細が表示されます。

- **名前:** ファンの名前。
- **ステータス:** ファンの状態。ERRORは期待値からの逸脱を示します。NAはファンが存在しないことを示します。
- **現在の値 (RPM):** 現在の1分あたりの回転数。

温度情報には、次の詳細が含まれます。

- **名前:** CPUやメモリモジュールなどのコンポーネントの名前 (例: P1-DIMM1A)。
- **ステータス:** コンポーネントの状態。ERRORは、現在の値が範囲外であることを示します。
- **現在の値 (摂氏):** コンポーネントの現在の温度 (摂氏)。

電圧情報には、次の詳細が含まれます。

- **名前:** CPUコアなど、コンポーネントの名前。
- **ステータス:** コンポーネントの状態。ERRORは、現在の値が範囲外であることを示します。
- **現在の値 (ボルト):** コンポーネントに存在する現在の電圧。

電源に関する情報には、次の詳細が含まれます。

- **名前:** コンポーネントの名前。
- **ステータス:** コンポーネントの状態。可能な値:
 - **エラー:** 電源が1つしか接続されていないか、動作していません。
 - **OK:** 両方の電源が接続されており、正常に動作しています。

SDXアプライアンスのインターフェースを監視する

SDXアプライアンスのインターフェースを監視し、必要に応じて是正措置を講じることができます。監視タブで、システムヘルスを展開し、インターフェースをクリックします。監視機能は、各インターフェースに関する次の情報を詳細に示します。

- **インターフェース:** SDXアプライアンス上のインターフェース番号。

- **ステータス:** インターフェースの状態。可能な値: UP、DOWN。
- **割り当て済みVF/合計:** インターフェースに割り当てられている仮想機能 (VF) の数と、そのインターフェースで利用可能な仮想機能の数。プラットフォームによってサポートされるVFの数は異なります。
- **送信パケット:** アプライアンスが最後に起動されてから送信されたパケットの数。
- **受信パケット:** アプライアンスが最後に起動されてから受信されたパケットの数。
- **Tx Bytes:** アプライアンスが最後に起動されてから送信されたバイト数。
- **Rx Bytes:** アプライアンスが最後に起動されてから受信されたバイト数。
- **Tx Errors:** アプライアンスが最後に起動されてからデータ送信中に発生したエラーの数。
- **Rx Errors:** アプライアンスが最後に起動されてからデータ受信中に発生したエラーの数。

システム通知設定の構成

多数のシステム関連機能について、選択したユーザーグループと通信するために通知を送信できます。SDX Management Serviceで通知サーバーを設定し、電子メールおよびショートメッセージサービス (SMS) ゲートウェイサーバーを構成して、ユーザーに電子メールおよびテキスト (SMS) 通知を送信できます。

注記

SDX Management Serviceリリース11.1にアップグレードすると、すべてのイベントカテゴリでシステム通知が有効になり、通知は既存の電子メールまたはSMSプロファイルに送信されます。

システム通知設定を構成するには

1. **System** \> **Notifications** \> **Settings** に移動し、**Change Notification Settings** をクリックします。
2. 「**システム通知設定の構成**」ページで、次の詳細を入力します。

- **カテゴリ** – SDX Management Serviceによって生成されるイベントのカテゴリ。 - **メール** – ドロップダウンメニューからメール配信リストを選択します。+ アイコンをクリックし、適切なフィールドに新しいメールサーバーの詳細を入力して、新しいメール配信リストを作成することもできます。 - **SMS (テキストメッセージ)** – ドロップダウンメニューからSMS配信リストを選択します。新しいSMS配信リストを作成するには、+ アイコンをクリックし、適切なフィールドに新しいSMSサーバーの詳細を入力します。

3. **OK** をクリックします。

Management Service から機能を有効化および無効化する

注

この機能は、リリース 13.1 ビルド 12.x 以降で利用可能です。

NetScaler SDX アプライアンスでは、Management Service がバックグラウンドで NetScaler インスタンスをポーリングし、SSL 証明書、ネットワーク機能、構成監査などの操作を行います。要件に応じて、このポーリングを有効または無効にするオプションが利用可能です。このポーリングを無効にすると、Management Service と ADC インスタンスのパフォーマンスが向上します。

GUI を使用して機能を有効または無効にするには

1. **System > System Settings** に移動します。
2. **Configure Features** をクリックします。
3. 機能を選択し、**Enable** または **Disable** をクリックします。

管理サービスを構成する

管理サービスを使用すると、クライアントセッションを管理したり、ユーザーアカウントの作成と管理、要件に応じたバックアップおよびプルーニングポリシーの調整などの構成タスクを実行したりできます。また、管理サービスを再起動したり、管理サービスのバージョンをアップグレードしたりすることもできます。さらに、管理サービスとCitrix Hypervisor™のtarファイルを作成し、テクニカルサポートに送信することもできます。

クライアントセッションを管理する

ユーザーが管理サービスにログオンすると、クライアントセッションが作成されます。アプライアンス上のすべてのクライアントセッションは、**セッションペイン**で表示できます。

セッションペインでは、次の詳細を表示できます。

- **ユーザー名:** セッションに使用されているユーザーアカウント。
- **IPアドレス:** セッションが作成されたクライアントのIPアドレス。
- **ポート:** セッションに使用されているポート。
- **ログイン時刻:** SDXアプライアンスで現在のセッションが作成された時刻。
- **最終アクティビティ時刻:** セッションでユーザーアクティビティが最後に検出された時刻。
- **セッションの有効期限:** セッションの有効期限が切れるまでの残り時間。

クライアントセッションを表示するには、**構成**タブで、**システム > セッション**に移動します。

クライアントセッションを終了するには、**セッションペイン**で、削除したいセッションをクリックし、**セッションの終了**をクリックします。

セッションを開始したクライアントからセッションを終了することはできません。

管理サービスのメモリを構成する

NetScaler SDXでは、Management Serviceメモリの85～90パーセントを占める可能性のある50～60個のVPXインスタンスをプロビジョニングできます。ハイエンドのNetScaler SDXでは、通常、より多くのメモリを消費する可能性のある120個以上のVPXインスタンスをプロビジョニングできます。デフォルトでは、Management Serviceメモリは2 GBです。バージョン14.1ビルド17.x以

降、Management Serviceメモリを3 GBまたは4 GBに増やすことができます。メモリの変更により、Management Serviceが再起動します。

前提条件

Management Serviceメモリを増やすには、SDX上に最低1 GBの追加の空きメモリが必要です。

NetScaler SDXの空きメモリを表示するには、**ダッシュボード**をクリックします。システムリソース使用率の下で、空きメモリを確認します。

例：

- メモリを3 GBに増やすには、少なくとも2 GBの空きメモリ（メモリを増やすための1 GBと追加の空きメモリ1 GB）が必要です。
- メモリを4 GBに増やすには、少なくとも3 GBの空きメモリ（メモリを増やすための2 GBと追加の空きメモリ1 GB）が必要です。

十分な空きメモリがない場合、エラーメッセージが表示されます。

Management Serviceメモリを構成するには

- 構成 > システム > システム設定 > Management Serviceメモリの構成に移動します。
- Management Serviceメモリの構成ページで、メモリリストから値を選択し、**保存**をクリックします。
- 確認メッセージボックスで、**はい**をクリックしてManagement Serviceを再起動します。

Management Serviceメモリのバックアップと復元

バージョン14.1ビルド21.x以降、Management Serviceメモリ設定のバックアップと復元が可能です。

Management Serviceメモリ（2 GB、3 GB、または4 GB）は、NetScaler SDXのバックアップ操作中にバックアップされます。同じメモリ値がNetScaler SDXの復元操作の一部として復元されます。

内部的に、管理サービスのメモリ復元は、管理サービスのメモリとバックアップ構成ファイルが異なる2つのメモリ値を持つ場合にのみ発生します。

ポリシーを構成する

ログデータのサイズを管理可能な制限内に保つため、SDXアプライアンスは指定された時間にバックアップおよびデータプルーニングポリシーを自動的に実行します。

プルーニングポリシーは毎日午前0時00分 to 01分 に実行され、アプライアンスに保持するデータの期間（日数）を指定します。デフォルトでは、アプライアンスは3日より古いデータを削除しますが、保持したいデータの期間（日数）を指定できます。イベントログ、監査ログ、タスクログのみが削除されます。

バックアップポリシーは毎日午前0時30分 to 01分 に実行され、ログと構成ファイルのバックアップを作成します。デフォルトでは、ポリシーは3つのバックアップを保持しますが、保持したいバックアップの数を指定できます。また、バックアップポリシーを使用して、次のことができます。

- バックアップファイルを暗号化します。
- SDXアプライアンスを構成して、FTP、SFTP、およびSCPを使用してバックアップファイルを外部バックアップサーバーに転送します。

ログデータを削除する日数を指定するには：

1. **Configuration** タブのナビゲーションペインで、**System** をクリックします。
2. **System** ペインの **Policy Administration** で、**Prune Policy** をクリックします。
3. **Modify Prune Policy** ダイアログボックスの **Data to keep (days)** で、アプライアンスが常に保持する必要があるデータの期間（日数）を指定します。
4. **OK** をクリックします。

バックアップポリシーを構成するには：

1. **Configuration** タブのナビゲーションペインで、**System** をクリックします。
2. **System** ペインの **Policy Administration** で、**Backup Policy** をクリックします。
3. 「バックアップポリシーの変更」ダイアログボックスの「保持する以前のバックアップ」で、アプライアンスが常に保持する必要があるバックアップの数を指定します。
4. バックアップファイルを暗号化するには、「バックアップファイルの暗号化」を選択します。
5. バックアップファイルを外部バックアップサーバーに転送するには、「外部転送」を選択し、次の操作を行います。
 - a. 「サーバー」フィールドに、外部バックアップサーバーのホスト名またはIPアドレスを入力します。

- b. 「ユーザー名」フィールドと「パスワード」フィールドに、外部バックアップサーバーにアクセスするためのユーザー名とパスワードを入力します。
 - c. 「ポート」フィールドに、ポート番号を入力します。
 - d. 「転送プロトコル」フィールドで、バックアップファイルを外部バックアップサーバーに転送するために使用するプロトコルを選択します。
 - e. 「ディレクトリパス」フィールドに、バックアップファイルを保存する外部バックアップサーバーのディレクトリのパスを入力します。
6. **転送後にManagement Serviceからファイルを削除する:** バックアップファイルを外部バックアップサーバーに転送した後、SDXアプライアンスからバックアップファイルを削除する場合は、このオプションを選択します。
7. 「OK」をクリックします。

Management Serviceを再起動する

システムペインからManagement Serviceを再起動できます。Management Serviceを再起動しても、インスタンスの動作には影響しません。Management Serviceの再起動プロセス中も、インスタンスは引き続き機能します。

Management Serviceを再起動するには:

1. **構成**タブのナビゲーションペインで、**システム**をクリックします。
2. システムペインの**システム管理**で、**Management Serviceの再起動**をクリックします。

Management Serviceファイルを削除する

SDXアプライアンスから不要なManagement Serviceのビルドファイルおよびドキュメントファイルを削除できます。

Management Serviceファイルを削除するには:

1. **Configuration**タブのナビゲーションペインで、**Management Service**を展開し、削除するファイルをクリックします。
2. **詳細**ペインで、ファイル名を選択し、**Delete**をクリックします。

テクニカルサポート用のtarアーカイブを生成する

テクニカルサポートオプションを使用して、Citrix®テクニカルサポートに提出するためのデータと統計のtarアーカイブを生成できます。このtarは、Management Service、Citrix Hypervisor、またはその両方に対して同時に生成できます。その後、ファイルをローカルシステムにダウンロードし、Citrixテクニカルサポートに送信できます。

テクニカルサポートペインで、次の詳細を表示できます。

- **名前：** tarアーカイブファイルの名前。ファイル名によって、tarがManagement Service用かCitrix Hypervisorサーバー用かが示されます。
- **最終変更日時：** このファイルが最後に変更された日付。
- **サイズ：** tarファイルのサイズ。

テクニカルサポート用のtarアーカイブを生成するには：

1. **Configuration**タブで、**Diagnostics > Technical Support**に移動します。
2. 詳細ペインの**Action**リストから、**Generate Technical Support File**を選択します。
3. **Generate Technical Support File**ダイアログボックスの**Mode**リストから、適切なオプションを選択します。
4. **OK**をクリックします。

テクニカルサポート用のtarアーカイブをダウンロードするには：

1. **Technical Support**ペインで、ダウンロードしたいテクニカルサポートファイルを選択します。
2. **Action**リストから**Download**を選択します。ファイルはローカルコンピューターに保存されます。

Management ServiceのCLIサポート

CLIを使用してManagement Serviceに対する操作を実行できるようになりました。以下の操作がサポートされています。

- **Add、Set、Delete** — リソースを設定するため。
- **Do** — システムレベルの操作を実行するため。例えば、Management Serviceのアップグレード、シャットダウン、または再起動など。
- **Save** — プロビジョニングに使用されるインターフェースを追加するため。

CLIにアクセスするには、Management ServiceのIPアドレスに接続された任意のワークステーションからセキュアシェル (SSH) クライアントを起動します。管理者資格情報を使用してログインします。

コマンドの使用法と構文に関する詳細情報は、manページからアクセスできます。

注記: CLIはコンソールアクセスではサポートされていません。

Management ServiceからのBMCアクセスを有効にする

注記:

LOMとBMCという単語は同じ意味で使用されます。

NetScaler®アプライアンスの一部には、アプライアンスのフロントパネルに、lights out management (LOM) ポートとしても知られるインテリジェントプラットフォーム管理インターフェイス (IPMI) が搭載されています。LOMは、ベースボード管理コントローラー (BMC) とも呼ばれます。LOMポートを使用すると、NetScalerソフトウェアとは独立して、アプライアンスをリモートで監視および管理できます。

データネットワークがダウンした場合でもアプライアンスへの接続を維持するために、BMC (LOM) ポートをデータチャネルとは別の専用チャネルに接続します。これにより、データケーブルとデータネットワークを単一障害点から排除できます。

ブラウザを介してBMC (LOM) ポートにアクセスし、ほとんどのタスクでGUIを使用できます。

管理サービスを使用してLOMアクセスを有効にする

1. 「**Configuration**」タブで、「**System**」に移動します。
2. 「**System Settings**」の下にある「**Configure BMC Settings**」をクリックします。

BMC設定の構成(/en-us/sdx/media/configure-bmc-settings.png)

3. BMC (LOM) のIPアドレス、サブネットマスク、およびデフォルトゲートウェイを指定します。MPX 9100およびMPX 16000では、これらのフィールドは**LOM Access**が**Unlocked**に設定されている場合にのみ編集可能です。**LOM Access**フィールドは他のプラットフォームでは利用できません。したがって、これらのフィールドはデフォルトで編集可能です。
4. 「**Save**」をクリックします。

認証および承認設定を構成する

NetScaler SDX Management Serviceでの認証は、ローカルまたは外部で行うことができます。外部認証の場合、Management Serviceは外部サーバーからの応答に基づいてユーザーアクセスを許可します。Management Serviceは、以下の外部認証プロトコルをサポートしています。

- リモート認証ダイヤルインユーザーサービス (RADIUS)
- ターミナルアクセスコントローラアクセス制御システム (TACACS)
- 軽量ディレクトリアクセスプロトコル (LDAP)

Management Serviceは、SSHからの認証要求もサポートしています。SSH認証は、キーボードインタラクティブ認証要求のみをサポートします。SSHユーザーの承認は、管理者権限のみに制限されています。読み取り専用権限を持つユーザーは、SSH経由でログオンできません。

認証を構成するには、認証タイプを指定し、認証サーバーを構成します。

Management Serviceを介した承認はローカルです。Management Serviceは2つのレベルの承認をサポートしています。管理者権限を持つユーザーは、Management Serviceで任意の操作を実行できます。読み取り専用権限を持つユーザーは、読み取り操作のみを実行できます。SSHユーザーの承認は、管理者権限のみに制限されています。読み取り専用権限を持つユーザーは、SSH経由でログオンできません。

Authorization for RADIUS and LDAP is supported by group extraction. You can set the group extraction attributes during the configuration of RADIUS or LDAP servers on the Management Service. The extracted group name is matched with the group names on the Management Service to determine the privileges given to the user. A user can belong to multiple groups. In that case, if any group to which the user belongs has admin privileges, the user has admin privileges. A Default Authentication group attribute can be set during configuration. This group is considered along with the extracted groups for authorization.

TACACS承認では、TACACSサーバー管理者は、管理者権限を持つユーザーに対して特別なコマンド「admin」を許可し、読み取り専用権限を持つユーザーに対してはこのコマンドを拒否する必要があります。ユーザーがSDXアプライアンスにログオンすると、Management Serviceはユーザーがこのコマンドを実行する権限を持っているかどうかを確認します。ユーザーが権限を持っている場合、ユーザーには管理者権限が割り当てられ、そうでない場合は読み取り専用権限が割り当てられます。

ユーザーグループを追加する

グループは、共通の情報にアクセスしたり、同様の種類のタスクを実行したりする必要があるユーザーの論理的な集合です。共通の操作のセットによって定義されたグループにユーザーを編成できます。個々のユーザーではなくグループに特定の権限を提供することで、ユーザー作成時の時間を節約できます。

認証に外部認証サーバーを使用している場合、SDXのグループは認証サーバーで構成されたグループと一致するように構成できます。認証サーバー上のグループと名前が一致するグループに属するユーザーがログオンして認証されると、そのユーザーはグループの設定を継承します。

ユーザーグループを追加するには

1. **Configuration > System > User Administration > Groups** に移動し、**Add** をクリックします。

(/en-us/sdx/media/system-group.png)

2. 「システムグループの作成」 ページで、次のパラメータを更新します。

- **グループ名:** グループの名前を入力します。使用できる文字は、英数字、アンダースコア (`_`)、ハッシュ (`#`)、ピリオド (`.`)、スペース、コロン (`:`)、アットマーク (`@`)、等号 (`=`)、ハイフン (`-`) です。最大長: 64。
- **グループの説明:** グループの簡単な説明を入力します。
- **システムアクセス:** SDXアプライアンス全体とその上で実行されているインスタンスへのアクセスを許可するオプションを選択します。または、インスタンスレベルのアクセスの場合、**すべてのインスタンスの下にあるインスタンス**を選択します。
- **権限:** リストからグループの権限を選択します。管理者は読み取り/書き込み権限を持っています。可能な値は次のとおりです。
 - **読み取り/書き込み:** グループは、管理サービスに関連するすべての管理タスクを実行できます。デフォルトでは、グループの権限は読み取り/書き込みに設定されています。
 - **読み取り:** グループはシステムを監視することのみができます。
- **ユーザーセッションタイムアウトの設定:** ユーザーがアクティブな状態を維持する期間を設定するオプションを選択します。

有効にすると、次のパラメータを指定できます。

- **セッションタイムアウト:** ユーザーセッションがアクティブな状態を維持できる期間を入力します。デフォルト値: 15。

- **セッションタイムアウト単位:** リストからタイムアウト単位を分または時間で選択します。デフォルト値: 分。

- **ユーザーセッション制限:** ユーザーごとに許可されるセッションの最大数を入力します。

注:

管理者グループおよび読み取り専用グループのメンバーには、デフォルトで40のユーザーセッションが割り当てられます。その他のグループのメンバーには、デフォルトで20のユーザーセッションが割り当てられます。

- **ユーザー:** グループに属するユーザーを一覧表示します。利用可能リストから選択し、**構成済み**リストに移動することで、ユーザーをグループに追加できます。

3. **作成**をクリックし、**閉じる**をクリックします。

ユーザーアカウントを構成する

ユーザーはアプライアンス管理タスクを実行するためにSDXアプライアンスにログオンします。ユーザーがアプライアンスにアクセスできるようにするには、そのユーザー用にSDXアプライアンス上にユーザーアカウントを作成する必要があります。ユーザーはアプライアンス上でローカルに認証されます。

重要: パスワードは SDXアプライアンス、Management Service、およびCitrix Hypervisorに適用されます。Citrix Hypervisor上で直接パスワードを変更しないでください。

ユーザーアカウントを構成するには

1. **構成**タブのシステムで、**管理**を展開し、**ユーザー**をクリックします。ユーザーペインには、既存のユーザーアカウントとその権限のリストが表示されます。
2. ユーザーペインで、次のいずれかを実行します。
 - ユーザーアカウントを作成するには、**追加**をクリックします。
 - ユーザーアカウントを変更するには、ユーザーを選択し、**変更**をクリックします。
3. システムユーザーの作成またはシステムユーザーの変更ダイアログボックスで、次のパラメータを設定します。
 - **名前*:** アカウントのユーザー名。名前に使用できる文字は、a～zおよびA～Zの文字、0～9の数字、ピリオド (.)、スペース、アンダースコア (_) です。最大長: 128。名前は変更できません。

- **パスワード***: アプライアンスにログオンするためのパスワード。最大長: 128
- **パスワードの確認***: パスワード。
- **権限***: アプライアンスでのユーザーの特権。可能な値:
 - **管理者**: ユーザーは、管理サービスに関連するすべての管理タスクを実行できます。
 - **読み取り専用**: ユーザーはシステムを監視し、アカウントのパスワードを変更することのみができます。デフォルト: 管理者。
- **外部認証を有効にする**: このユーザーの外部認証を有効にします。管理サービスは、データベースユーザー認証の前に外部認証を試行します。このパラメーターが無効になっている場合、ユーザーは外部認証サーバーで認証されません。 **注**: リモート認証サーバーに到達できない場合、ユーザーはアプライアンスへのアクセスを失う可能性があります。そのような場合、認証はデフォルトの管理者ユーザー (`nsroot`) にフォールバックします。
- **セッションタイムアウトの設定**: ユーザーがアクティブな状態を維持できる期間を設定できます。次の詳細を指定します。
 - **セッションタイムアウト**: ユーザーセッションがアクティブな状態を維持できる期間。
 - **セッションタイムアウト単位**: タイムアウト単位 (分または時間)。
- **グループ**: ユーザーにグループを割り当てます。

*必須パラメーター

4. 作成またはOKをクリックし、次に閉じるをクリックします。作成したユーザーは、ユーザーペインに表示されます。

ユーザーアカウントを削除するには

1. **構成**タブで、ナビゲーションペインの**システム**を展開し、**管理**を展開し、次に**ユーザー**をクリックします。
2. **ユーザー**ペインで、ユーザーアカウントを選択し、次に**削除**をクリックします。
3. 確認メッセージボックスで、**OK**をクリックします。

認証タイプを設定する

管理サービスインターフェイスから、ローカル認証または外部認証を指定できます。外部認証は、デフォルトでローカルユーザーに対して無効になっていますが、ローカルユーザーを追加する際、またはユーザーの設定を変更する際に、オプションをオンにすることで有効にできます。

重要: 外部認証は、RADIUS、LDAP、またはTACACS認証サーバーを設定した後にのみサポートされます。

認証タイプを設定するには

1. 「**Configuration**」 タブで、「**System**」の下にある「**Authentication**」をクリックします。
2. 詳細ペインで、「**Authentication Configuration**」をクリックします。
3. 次のパラメータを設定します。
 - **サーバータイプ**: ユーザー認証用に構成された認証サーバーのタイプ。指定可能な値：LDAP、RADIUS、TACACS、およびローカル。
 - **サーバー名**: Management Serviceで構成された認証サーバーの名前。メニューには、選択した認証タイプ用に構成されたすべてのサーバーが表示されます。
 - **フォールバックローカル認証を有効にする**: 代替として、外部認証が失敗した場合にローカル認証でユーザーを認証することもできます。このオプションはデフォルトで有効になっています。
4. 「OK」をクリックします。

基本認証を有効または無効にする

基本認証を使用して、Management Service NITROインターフェイスに認証できます。デフォルトでは、SDXアプライアンスで基本認証が有効になっています。Management Serviceインターフェイスを使用して基本認証を無効にするには、次の手順を実行します。

基本認証を無効にするには

1. 「**Configuration**」 タブで、「**System**」をクリックします。
2. 「**System Settings**」グループで、「**Change System Settings**」をクリックします。
3. 「Configure System Settings」ダイアログボックスで、「**Allow Basic Authentication**」チェックボックスをオフにします。
4. **OK** をクリックします。

外部認証サーバーの構成

NetScaler SDX Management Serviceは、ローカルユーザーアカウントまたは外部認証サーバーを使用してユーザーを認証できます。アプライアンスは次の認証タイプをサポートしています。

- **ローカル** — 外部認証サーバーを参照せずに、パスワードを使用してManagement Serviceに認証します。ユーザーデータはManagement Serviceにローカルに保存されます。
- **RADIUS** — 外部RADIUS認証サーバーに認証します。
- **LDAP** — 外部LDAP認証サーバーに認証します。

- TACACS — 外部のTerminal Access Controller Access-Control System (TACACS) 認証サーバーに認証します。

外部認証を構成するには、認証タイプを指定し、認証サーバーを構成します。

RADIUSサーバーの追加

RADIUS認証を構成するには、認証タイプをRADIUSとして指定し、RADIUS認証サーバーを構成します。

Management Serviceは、RADIUS仕様に従ってRADIUSチャレンジレスポンス認証をサポートしています。RADIUSユーザーは、RADIUSサーバーでワンタイムパスワードを設定できます。ユーザーがSDXアプライアンスにログオンすると、このワンタイムパスワードの指定を求められます。

RADIUSサーバーを追加するには

1. **Configuration**タブで、**System**の下にある**Authentication**を展開し、**Radius**をクリックします。
2. 詳細ペインで、**Add**をクリックします。
3. **Create Radius Server**ダイアログボックスで、パラメーターの値を入力または選択します。

- 名前* — サーバーの名前。
- サーバー名 / IPアドレス*—完全修飾ドメイン名 (FQDN) またはサーバーIPアドレス。 **注:** DNSは指定されたFQDNをIPアドレスに解決できる必要があります、FQDNの解決にはプライマリDNSのみが使用されます。プライマリDNSを手動で設定するには、「FQDN名前解決用のプライマリDNSの追加」セクションを参照してください。
- ポート*—RADIUSサーバーが稼働しているポート。デフォルト値: 1812。
- タイムアウト*—システムがRADIUSサーバーからの応答を待機する秒数。デフォルト値: 3。
- シークレットキー*—クライアントとサーバー間で共有されるキー。この情報は、システムとRADIUSサーバー間の通信に必要です。
- NAS IPアドレス抽出を有効にする—有効にすると、RADIUSプロトコルに従って、管理サービスIPアドレスが `nasip` としてサーバーに送信されます。
- NASID—設定されている場合、この文字列はRADIUSプロトコルに従って `nasid` としてRADIUSサーバーに送信されます。
- グループプレフィックス—RADIUSグループ抽出のために、RADIUS属性内のグループ名の前に付加されるプレフィックス文字列。
- グループベンダーID—RADIUSグループ抽出に使用するベンダーID。

- グループ属性タイプ—RADIUSグループ抽出の属性タイプ。
- グループセパレーター—RADIUSグループ抽出のために、RADIUS属性内のグループ名を区切るグループセパレーター文字列。
- IPアドレスベンダー識別子—イントラネットIPを示すRADIUS属性のベンダーID。値が0の場合、属性はベンダーエンコードされていないことを示します。
- IPアドレス属性タイプ—RADIUS応答におけるリモートIPアドレス属性の属性タイプ。
- パスワードベンダー識別子—RADIUS応答におけるパスワードのベンダーID。ユーザーパスワードの抽出に使用されます。
- パスワード属性タイプ—RADIUS応答におけるパスワード属性の属性タイプ。
- パスワードエンコーディング—システムからRADIUSサーバーへ送信されるRADIUSパケットでパスワードをエンコードする方法。指定可能な値: pap、chap、mschapv1、および mschapv2。
- デフォルト認証グループ—認証が成功した際に、抽出されたグループに加えて選択されるデフォルトのグループ。
- アカウンティング—RADIUSサーバーで監査情報をログに記録するように管理サービスを有効にします。

4. 「作成」をクリックし、次に「閉じる」をクリックします。

LDAP認証サーバーの追加

LDAP認証を設定するには、認証タイプをLDAPとして指定し、LDAP認証サーバーを設定します。

LDAPサーバーを追加するには

1. 「**Configuration**」タブの「**System**」で、「**Authentication**」を展開し、「**LDAP**」をクリックします。
2. 詳細ペインで、「**追加**」をクリックします。
3. 「LDAPサーバーの作成」ダイアログボックスで、パラメーターの値を入力または選択します。
 - 名前*—サーバーの名前。
 - サーバー名/IPアドレス*—FQDNまたはサーバーのIPアドレス。**注:** DNSは指定されたFQDNをIPアドレスに解決できる必要があります、FQDNの解決にはプライマリDNSのみが使用されます。プライマリDNSを手動で設定するには、「FQDN名前解決のためのプライマリDNSの追加」セクションを参照してください。
 - ポート*—LDAPサーバーが稼働しているポート。デフォルト値: 389。

- タイムアウト*—システムがLDAPサーバーからの応答を待機する秒数。
- ベースDN—LDAP検索を開始する必要があるベース、またはノード。
- タイプ—LDAPサーバーのタイプ。可能な値: Active Directory (AD) および Novell Directory Service (NDS)。
- Administrative Bind DN—LDAPサーバーにバインドするために使用される完全識別名。
- Administrative Password—LDAPサーバーにバインドするために使用されるパスワード。
- Validate LDAP Certificate—LDAPサーバーから受信した証明書を検証するには、このオプションをオンにします。
- LDAP Host Name—LDAPサーバーのホスト名。validateServerCertパラメーターが有効になっている場合、このパラメーターはLDAPサーバーからの証明書上のホスト名を指定します。ホスト名が一致しない場合、接続エラーが発生します。
- Server Logon Name Attribute—システムが外部LDAPサーバーまたはActive Directoryを照会するために使用する名前属性。
- Search Filter—デフォルトのLDAPユーザー検索文字列と組み合わせて値を形成する文字列。例えば、ldaploginame `samaccount` とユーザーが指定したユーザー名 bob を持つ `vpnallowed=true` は、LDAP検索文字列 `(&(vpnallowed=true)(samaccount=bob))` を生成します。
- Group Attribute—LDAPサーバーからのグループ抽出のための属性名。
- Sub Attribute Name—LDAPサーバーからのグループ抽出のためのサブ属性名。
- Security Type—アプライアンスと認証サーバー間の通信に使用する暗号化の種類。指定可能な値:

PLAINTEXT: 暗号化は不要です。

TLS: TLSプロトコルを使用して通信します。

SSL: SSLプロトコルを使用して通信します。

- Default Authentication Group—抽出されたグループに加えて、認証が成功したときに選択されるデフォルトグループ。
- Referrals—LDAPサーバーから受信したLDAPリフェラルの追跡を有効にします。
- Maximum LDAP Referrals—追跡するLDAPリフェラルの最大数。
- パスワード変更を有効にする — パスワードの有効期限が切れた場合に、ユーザーがパスワードを変更できるようにします。パスワードは、設定されているセキュリティタイプが TLSまたはSSLの場合にのみ変更できます。

- ネストされたグループの抽出を有効にする — ネストされたグループの抽出機能を有効にします。
- 最大ネストレベル — グループ抽出が許可されるレベルの数。
- グループ名識別子 — LDAPサーバーでグループを一意に識別する名前。
- グループ検索属性 — LDAPグループ検索属性。グループがどのグループに属するかを判断するために使用されます。
- グループ検索サブ属性 — LDAPグループ検索サブ属性。グループがどのグループに属するかを判断するために使用されます。
- グループ検索フィルター — デフォルトのLDAPグループ検索文字列と組み合わせて検索値を形成する文字列。

4. 作成をクリックし、次に閉じるをクリックします。

LDAPユーザーのSSH公開鍵認証サポート

SDXアプライアンスは、ログオン時にSSH公開鍵認証を介してLDAPユーザーを認証できるようになりました。公開鍵のリストは、LDAPサーバーのユーザーオブジェクトに保存されます。認証中に、SSHはLDAPサーバーからSSH公開鍵を抽出します。取得された公開鍵のいずれかがSSHをサポートしている場合、ログオンは成功します。

抽出された公開鍵の同じ属性名が、LDAPサーバーとNetScaler SDXアプライアンスの両方に存在する必要があります。

重要

キーベース認証の場合、`/etc/sshd_config` ファイル内の `Authorizedkeysfile` の値を設定して、次の観点から公開鍵の場所を指定する必要があります。

`AuthorizedKeysFile .ssh/authorized_keys`

システムユーザー。 `/etc/sshd_config` * ファイル内の `Authorizedkeysfile`` の値を設定することで、任意のシステムユーザーの公開鍵の場所を指定できます。

LDAPユーザー。 取得された公開鍵は、`/var/pubkey/<user_name>/tmp_authorized_keys-<pid>` ディレクトリに保存されます。`pid` は、同じユーザーからの同時SSHリクエストを区別するために追加される一意の番号です。この場所は、認証プロセス中に公開鍵を保持するための一時的な場所です。認証が完了すると、公開鍵はシステムから削除されます。

ユーザーとしてログインするには、シェルスクリプトから次のコマンドを実行します。

```
$ ssh -i <private key> <username>@<IPAddress>
```

GUIを使用してLDAPサーバーを構成するには:

1. **System > Authentication > LDAP** に移動します。
2. LDAPページで、タブをクリックします。
3. 利用可能なLDAPサーバーのいずれかをクリックします。
4. **Configure Authentication LDAP Server** ページで、**Authentication** を選択します。



注:

LDAPユーザーの認証に「sshPublicKeys」を使用するには、チェックボックスをオフにします。

FQDN名前解決のためのプライマリDNSの追加

サーバーのIPアドレスの代わりにFQDNを使用してRADIUSまたはLDAPサーバーを定義する場合、サーバー名を解決するためにプライマリDNSを手動で設定します。GUIまたはCLIのいずれかを使用できます。

GUIを使用してプライマリDNSを設定するには、**System > Network Configuration > DNS** に移動します。

CLIを使用してプライマリDNSを設定するには、次の手順に従います。

1. Secure Shell (SSH) コンソールを開きます。
2. 管理者資格情報を使用して、NetScaler SDX アプライアンスにログオンします。
3. `networkconfig` コマンドを実行します。
4. 適切なメニューを選択し、DNS IPv4アドレスを更新して、変更を保存します。

再度 `networkconfig` コマンドを実行すると、更新されたDNSアドレスが表示されます。

TACACSサーバーの追加

TACACS認証を構成するには、認証タイプをTACACSとして指定し、TACACS認証サーバーを構成します。

TACACSサーバーを追加するには

1. **Configuration** タブで、**System** の下にある **Authentication** を展開し、**TACACS** をクリックします。
2. 詳細ペインで、**Add** をクリックします。
3. 「Create TACACS Server」ダイアログボックスで、パラメーターの値を入力または選択します。

- 名前 — TACACSサーバーの名前
- IPアドレス — TACACSサーバーのIPアドレス
- ポート — TACACSサーバーが実行されているポート。デフォルト値: 49
- タイムアウト — システムがTACACSサーバーからの応答を待機する最大秒数
- TACACSキー — クライアントとサーバー間で共有されるキー。この情報は、システムがTACACSサーバーと通信するために必要です。
- アカウンティング — 管理サービスがTACACSサーバーで監査情報をログに記録できるようにします。
- グループ属性名 — TACACS+サーバーで構成されたグループ属性の名前。

TACACSサーバーの作成(/en-us/sdx/media/create-tacacs-server.png)

4. **作成**をクリックし、次に**閉じる**をクリックします。

Management Serviceからリンクアグリゲーションを構成する

リンクアグリゲーションは、複数のイーサネットリンクを1つの高速リンクに結合します。リンクアグリゲーションを構成すると、NetScaler SDXアプライアンスと他の接続デバイス間の通信チャネルの容量と可用性が向上します。集約されたリンクは「チャネル」とも呼ばれます。

ネットワークインターフェイスがチャネルにバインドされている場合、チャネルパラメータはネットワークインターフェイスパラメータよりも優先されます。(つまり、ネットワークインターフェイスパラメータは無視されます。) ネットワークインターフェイスは1つのチャネルにのみバインドできます。

ネットワークインターフェイスがチャネルにバインドされると、そのVLAN構成は破棄されます。インターフェイスは元々属していたVLANから削除され、デフォルトVLANに追加されます。ただし、チャネルを元のVLANまたは新しいVLANに再度バインドできます。たとえば、ネットワークインターフェイス1/2と1/3をID 2のVLAN (VLAN 2) にバインドし、その後それらをチャネルLA/1

にバインドすると、ネットワークインターフェイスはデフォルトVLANに移動しますが、チャンネルをVLAN 2にバインドできます。

注:

- インターフェイスは1つのチャンネルの一部である必要があります。
- チャンネルを構成するには、最低2つのインターフェイスが必要です。
- チャンネルの一部を構成するインターフェイスは、NetScalerインスタンスを追加または変更する際に、ネットワーク設定ビューには表示されません。インターフェイスの代わりに、チャンネルが一覧表示されます。

1つのインスタンスに割り当てられた3つのインターフェイスを使用してチャンネルを構成し、2番目のインスタンスがこれらのインターフェイスの一部を使用する場合、Management Serviceは2番目のインスタンスをシャットダウンし、ネットワーク設定を変更して、インスタンスを再起動します。たとえば、Instance1とInstance2という2つのインスタンスがあるとします。これらのインスタンスがプロビジョニングされると、インターフェイス10/1、10/2、および10/3はInstance1に割り当てられ、インターフェイス10/1および10/2はInstance2に割り当てられます。インターフェイス10/1、10/2、および10/3でLAチャンネルが作成された場合、instance1は再起動されません。ただし、Management ServiceはInstance2をシャットダウンし、インターフェイス10/3をInstance2に割り当ててから、Instance2を再起動します。

LAチャンネルからインターフェイスを削除すると、変更はデータベースに保存され、インスタンスを追加または変更する際に、ネットワーク設定ビューにインターフェイスが表示されます。インターフェイスを削除する前は、インターフェイスが属するチャンネルのみが一覧表示されます。

Management Service からチャンネルを構成する

チャンネルは手動で構成することも、Link Aggregation Control Protocol (LACP) を使用することもできます。LACP を手動で構成されたチャンネルに適用することはできません。また、LACP によって作成されたチャンネルを手動で構成することもできません。Management Service からチャンネルを構成します。その後、NetScaler インスタンスのプロビジョニング時または変更時にチャンネルを選択します。

LAチャンネルは、リンク冗長性と帯域幅集約を提供するための論理エンティティです。チャンネルの一部であるインターフェイスには、個別のIPアドレスを割り当てることはできません。

注: NetScaler SDXアプライアンスはリンクアグリゲーションをサポートしますが、リンク冗長性はサポートしません。NetScalerリリース13.1ビルド27.x以降では、NetScaler SDXアプライアンスでホストされているNetScaler VPXインスタンスでのリンク冗長性構成は明示的にサポートされていません。

Management Service からチャネルを構成するには

1. **System > Channels** に移動します。
2. 詳細ペインで、**Add** をクリックします。
3. **Add Channel** ダイアログボックスで、次のパラメータを設定します。
 - **チャンネルID** — 作成するLAチャネルのID。LA/x 表記でLAチャネルを指定します。ここで、x はインターフェイス数の半分に等しい数まで1から指定できます。LAチャネルの作成後は変更できません。
 - **タイプ** — チャネルのタイプ。可能な値:
 - **Static** — データインターフェイスのみで構成されます。
 - **アクティブ-アクティブ** — 管理インターフェイス 0/x でのみ構成されます。
 - **アクティブ-パッシブ** — 管理インターフェイス 0/x でのみ構成されます。
 - **LACP** — データインターフェイスと管理インターフェイス0/xで構成されます。
 - **スループット** (静的チャネルとLACPにのみ適用) — LAチャネルのスループットの低しきい値 (Mbps)。HA構成では、LAチャネルでHA MONが有効になっており、スループットが指定されたしきい値を下回ると、フェイルオーバーがトリガーされます。
 - **帯域幅高** (静的チャネルおよびLACPにのみ適用)—LAチャネルの帯域幅使用量に対する高しきい値 (Mbps単位)。LAチャネルの帯域幅使用量が指定された高しきい値以上になると、アプライアンスはSNMPトラップメッセージを生成します。
 - **帯域幅正常** (静的チャネルおよびLACPにのみ適用)—LAチャネルの帯域幅使用量に対する正常しきい値 (Mbps単位)。LAチャネルの帯域幅使用量が高しきい値を超えた後、指定された正常しきい値以下になると、NetScaler SDXアプライアンスは帯域幅使用量が正常に戻ったことを示すSNMPトラップメッセージを生成します。
4. **インターフェイス**タブで、このチャネルに含めるインターフェイスを追加します。
5. **設定**タブで、次のパラメータを設定します。
 - **チャネルの状態** (静的チャネルにのみ適用)—LAチャネルを有効または無効にします。
 - **LACP時間** (LACPにのみ適用)—LACPDUを受信しない場合に、リンクが集約されない時間。この値は、SDXアプライアンスとパートナーノードのリンクアグリゲーションに参加しているすべてのポートで一致する必要があります。
 - **HA監視**—High Availability (HA) 構成では、チャネルの障害イベントを監視します。HA MONが有効になっているLAチャネルの障害は、HAフェイルオーバーをトリガーします。

- すべてタグ付け—このチャンネルで送信されるすべてのパケットに4バイトの802.1qタグを追加します。ON設定は、このチャンネルにバインドされているすべてのVLANにタグを適用します。OFF設定は、ネイティブVLAN以外のすべてのVLANにタグを適用します。
- エイリアス名—LAチャンネルのエイリアス名。読みやすさを向上させるためにのみ使用されます。何らかの操作を実行するには、LAチャンネルIDを指定する必要があります。

6. **作成**をクリックし、次に**閉じる**をクリックします。

注

- 0/1および0/2インターフェイスの両方がVPXインスタンスの一部であり、そのインスタンスがクラスターの一部である場合、管理LAを作成することはできません。
- 管理LAがVPXインスタンスの一部であり、そのインスタンスがクラスターの一部である場合、管理LAを削除することはできません。

アクセス制御リスト

アクセス制御リスト (ACL) は、IP トラフィックをフィルタリングし、不正アクセスからアプライアンスを保護するために、ネットワークアプライアンスに適用できる一連の条件です。

NetScaler SDX Management Service GUI で ACL を構成して、アプライアンスへのアクセスを制限および制御できます。

注:

SDX アプライアンスの ACL は、リリース 12.0 57.19 以降でサポートされています。

このトピックには、次のセクションが含まれています。

- 使用ガイドライン
- ACL の構成方法
- ACL ルールに対するその他のアクション
- トラブルシューティング

使用ガイドライン

アプライアンスで ACL を作成する際は、次の点に留意してください。

- SDX アプライアンスをリリース 11.0 57.19 にアップグレードすると、ACL 機能はデフォルトで無効になります。
- SDX 管理者は、SDX アプライアンス上の ACL を介してインバウンドパケットのみを制御できます。
- NetScaler Console を使用して SDX アプライアンスを管理する場合は、MAS と SDX Management Service 間の通信を許可するために、適切な ACL ルールを作成する必要があります。
- SDXアプライアンス上のVPXのプロビジョニングまたは削除、外部サーバーの追加/削除、SNMP管理などのその他の設定では、既存のACL構成を変更する必要はありません。これらのエンティティとの通信は、管理サービスによって処理されます。

ACLを構成する方法

ACLの構成には、次の手順が含まれます。

- ACL機能を有効にする
- ACLルールを作成する
- ACLルールを有効にする

注:

ACL機能を有効にせずにACLルールを作成できます。ただし、機能が有効になっていない場合、作成後にACLルールを有効にすることはできません。

ACL機能を有効にする

1. ACL機能を有効にするには、SDX管理サービスGUIにログオンし、**構成 > システム > ACL**に移動します。
2. トグルボタンを使用して、ACL機能をオンにします。

ACLルール(/en-us/sdx/media/sdx-acl-1.png)

ACLルールを作成する

1. ACLページで、**ルールの作成**をクリックします。
2. **ルールの作成**ウィンドウが開きます。次の表に記載されている詳細を追加します。

|プロパティ|説明| |--| |名前|名前を追加します。||プロトコル|メニューからプロトコルを選択します。デフォルトでは、TCPが選択されています。すべてのプロトコルを許可するには、

ANYを選択します。||送信元IPアドレス/サブネット|ルールが適用される送信元IPアドレスまたは送信元サブネットを指定します。すべての受信トラフィックにルールを適用する必要がある場合は、**ANY**を選択します。||宛先IP|SDX管理サービスのIPアドレスは、宛先IPとして自動入力されます。このフィールドは編集できません。||宛先ポート|ルールが適用される宛先ポートを指定します。すべての宛先ポートにルールを適用する場合は、**ANY**を選択します。||アクション|ルールの動作（許可または拒否）を選択します。||優先度|ルールが評価される順序を指定するために優先度を割り当てます。優先度番号は、着信パケットに対してACLルールが照合される順序を決定します。優先度番号が小さいほど、優先度が高くなります。例えば、優先度番号1は優先度番号1よりも優先度が高いです。いずれのルールも着信パケットと一致しない場合、そのパケットはブロックされます。|

3. ルールを作成するには、**OK**をクリックします。

図: ACLルールの例

SDX ACLルール(/en-us/sdx/media/example-sdx-acl-rule.png)

ルールが作成されると、無効な状態になります。ルールを有効にするには、ルールを有効にする必要があります。

注:

ルールを有効にするには、ACL機能が有効になっている必要があります。この機能が無効な状態でACLルールを有効にしようとすると、「ACL is not running」というメッセージが表示されます。

ACLルールを有効にする

1. 有効にしたいルールにマウスカーソルを合わせ、3つの点がある円をクリックします。
2. メニューから、**有効にする**を選択します。
3. または、そのルールのラジオボタンを選択し、**有効にする**タブをクリックします。
4. プロンプトが表示されたら、**はい**をクリックして確定します。

ACLルールのその他のアクション

ACLルールには、次のアクションを適用できます。

1. ACLルールを無効にする
2. ACLルールを編集する
3. ACLルールを削除する

4. ACLルール of 優先順位を振り直す

ACLルールを無効にする

1. 無効にしたいルールにマウスカーソルを合わせ、3つの点がある円を選択します。
2. リストから**無効にする**をクリックします。
3. または、そのルールのラジオボタンを選択し、**無効にする**タブをクリックします。
4. 確認のため**はい**をクリックします。

注:

ルールを無効にすると、そのルールは受信トラフィックに適用されなくなります。ただし、ルール of 設定はACL設定の下に残ります。

ACLルールを編集する

1. 編集したいルールにマウスカーソルを合わせ、3つの点がある円を選択します。
2. リストから**ルール of 編集**をクリックします。ルール of 変更ウィンドウが開きます。
3. または、そのルールのラジオボタンを選択し、**ルール of 編集**タブをクリックします。ルール of 変更ウィンドウが開きます。
4. 編集を行い、**OK**をクリックします。

注記:

ルールは、有効状態と無効状態 of 両方で編集できます。すでに有効になっているルールを編集した場合、変更はすぐに適用されます。無効状態 of ルール of 場合、変更はルールを有効にしたときに適用されます。

ACLルールを削除する

1. ルールが無効状態であることを確認します。
2. 削除したいルールにマウスを重ね、3つの点がある円を選択します。リストから**Delete Rule**をクリックします。
3. または、そのルールのラジオボタンを選択し、**Delete Rule**タブをクリックします。
4. **Yes**をクリックして確定します。

注記:

有効状態のルールは削除できません。

ACLルールの優先順位を振り直す

1. 優先順位を振り直したいルールにマウスを重ね、3つの点がある円を選択します。リストから ****Renumber Priority(s)**** をクリックします。
2. または、そのルールのラジオボタンを選択し、**Select Action** タブをクリックします。
3. ****Renumber Priority(s)**** を選択します。
4. SDX Management Serviceは、既存のすべてのルールに、10の倍数である新しい優先順位番号を自動的に割り当てます。
5. 要件に応じて優先順位番号を割り当てるためにルールを編集します。ルールの編集方法の詳細については、「ACLルールを編集するには」セクションを参照してください。

既存の優先度番号の例



優先度を再番号付けした後の、10の倍数で表された優先度番号の例



トラブルシューティング

ACLルールが不適切に設定されていると、すべてのユーザーアカウントがアクセスを拒否される可能性があります。ACLの設定が不適切であったために、誤ってSDX Management Serviceへのネットワークアクセスをすべて失った場合は、次の手順に従ってアクセスを回復してください。

1. SSHと「root」アカウントを使用して、Citrix Hypervisor™管理IPアドレスにログオンします。
2. 管理者権限を使用して、Management Service VMのコンソールにログオンします。
3. コマンド `pfctl -d` を実行します。
4. GUIからManagement Serviceにログオンし、ACLを適切に再構成します。

NetScalerインスタンスのクラスターをセットアップする

1つ以上のSDXアプライアンスにNetScalerインスタンスをプロビジョニングした後、NetScalerインスタンスのクラスターを作成できます。

Citrix®は、クラスター構成をManagement Serviceから実行することを推奨しています。VPXインスタンスからクラスター構成を実行すると、Management Serviceは30分ごとの自動検出中に構成を学習します。最悪の場合、クラスタリング情報は30分間検出されません。クラスターは正常に機能する可能性があります。クラスターの依存関係に関するいくつかの重要な検証チェックが見落とされます。Management Serviceは、ADCインスタンスでクラスターを構成する前にこれらのチェックを実行します。したがって、すべてのクラスター構成はManagement Serviceから実行する必要があります。

注:

- クラスターをセットアップするには、NetScalerクラスタリングを理解する必要があります。詳細については、「[クラスタリング](#)」を参照してください。
- SDXアプライアンス全体にNetScalerインスタンスを持つクラスターの場合、Citrixは3つのSDXアプライアンスからNetScalerインスタンスを使用することを推奨しています。このプロセスにより、最小 $(n/2 + 1)$ ノードというクラスター基準が常に満たされることが保証されます。

図1. SDX NetScalerインスタンスのクラスター



上の図は、同じサブネット上にある3つのSDXアプライアンス（SDX1、SDX2、SDX3）を示しています。これらのアプライアンス上のNetScalerインスタンスは、Cluster1とCluster2の2つのクラスターを形成するために使用されます。

- Cluster1には、SDX1上の2つのインスタンスが含まれます。
- Cluster2には、SDX1上の1つのインスタンス、SDX2上の2つのインスタンス、およびSDX3上のさらに2つのインスタンスが含まれます。

留意事項

- クラスターの各ノードには6 GBのRAMを使用することをお勧めします。
- NetScaler SDX™ アプライアンスでホストされているNetScaler VPXインスタンスには、専用のコアをプロビジョニングする必要があります。
- Mellanoxインターフェイス（50Gおよび100G）を使用したCLAG形成は、SDXプラットフォームではサポートされていません。
- クラスターのすべてのノードは同じタイプである必要があります。以下の組み合わせでクラスターを形成することはできません。
 - ハードウェアアプライアンスと仮想アプライアンス。

- NetScaler VPXインスタンスとNetScaler SDXインスタンス。
- 異なるSDXハードウェアプラットフォーム上のADCインスタンス。
- NetScalerインスタンスはすべて同じバージョンである必要があり、バージョン10.1以降である必要があります。
- NetScalerインスタンスはすべて同じ機能ライセンスを持っている必要があります。
- クラスターに追加された後、個々のNetScalerインスタンスで構成を更新することはできません。すべての変更はクラスターIPアドレスを介して実行する必要があります。
- NetScalerインスタンスはすべて同じリソース（メモリ、CPU、インターフェイスなど）を持っている必要があります。
- バックプレーンMTUは、データインターフェイスMTUより78バイト大きくする必要があります。
- データインターフェイスMTUが9138バイト以内であることを確認してください。
- リリース13.0ビルド82.x以降では、ノードをクラスターに追加する際にSNIPアドレスを追加するよう求められます。ノードの追加中にSNIPアドレスを動的に作成することもできます。この機能は、厳密な送信元IPアドレスチェックに関するセキュリティ問題に対処するのに役立ちます。
- **重要！** クラスターの削除オプションは注意して使用してください。クラスターの削除をクリックすると、警告なしにクラスターが削除されます。

SDXアプライアンスでクラスターをセットアップする

1. SDXアプライアンスにログオンします。
2. **Configuration**タブで、**NetScaler > Clusters > Cluster Instances**に移動します。
3. クラスターを作成します:
 - a. **Create Cluster** をクリックします。
 - b. **Create Cluster** ダイアログボックスで、クラスターに必要なパラメーターを設定します。パラメーターの説明については、対応するフィールドにマウスポインターを合わせます。
 - c. 構成の概要を表示するには、**Next** をクリックします。
 - d. **Finish** をクリックしてクラスターを作成します。注: L2 VLANが構成されたNetScalerインスタンスがクラスターに追加されると、add VLANコマンドは `sdxvlan` パラメーターがYesに設定された状態で保存されます。このパラメーターは内部引数であり、SDXクラスター形成中の接続損失を回避するために使用されます。
4. クラスターにノードを追加します:

- a. **Add Node** をクリックします。
- b. **Add Node** ダイアログボックスで、クラスターノードの追加に必要なパラメーターを設定します。パラメーターの説明については、対応するフィールドにマウスポインターを合わせます。
- c. 構成の概要を表示するには、**Next** をクリックします。
- d. **Finish** をクリックしてノードをクラスターに追加します。
- e. 手順1から4を繰り返して、別のノードをクラスターに追加します。

クラスターを作成した後、クラスターIPアドレスを介してアクセスし、構成する必要があります。

クラスターインスタンス内のノードが同じCitrix NetScaler SDXアプライアンスに属している場合、NetScaler SDXアプライアンスが故障すると、クォーラムを失う可能性があります。

以下の方法でクラスターノードを展開できます：

1. 各NetScaler SDXアプライアンスから1つのVPXインスタンスを使用して、複数のクラスターインスタンスを作成します。

例：

SDX1	SDX2	INSTANCEID
VPX1	VPX1	1
VPX2	VPX2	2

1. NetScaler SDXアプライアンスが2台を超える場合は、**quorumType Majority** を使用して、すべてのアプライアンスのVPXインスタンスで単一のクラスターインスタンスを作成します。この場合、VPXインスタンスがすべてのNetScaler SDXアプライアンスに均等に分散されていることを確認してください。

例1：

SDX1	SDX2	SDX3	インスタンスID
VPX1	VPX1	VPX1	1
VPX2	VPX2	VPX2	NA
VPX3	VPX3	VPX3	NA

例2：

SDX1	SDX2	SDX3	インスタンスID
VPX1	VPX1	VPX1	1
VPX2	VPX2	VPX2	N/A
VPX3	VPX3	VPX3	N/A
VPX4	NA	NA	NA

1. すべてのNetScaler SDXデバイスのすべてのVPXインスタンスを含む単一のクラスターインスタンスを作成します。ただし、`quorum type NONE` を使用してください。これにはいくつかの制限があります。

例:

SDX1	SDX2	INSTANCEID
VPX1	VPX1	1
VPX2	VPX2	2
VPX3	NA	NA

-quorumType パラメータが **NONE** に設定されている場合の制限事項：

- 単一障害点によるネットワークパーティションを回避するため、トポロジはクラスターノード間に冗長リンクを持つ必要があります。
- ノードの追加や削除などのクラスター操作中に、クラスターが不安定になる可能性があります。

注：

SDXアプライアンスのNetScalerインスタンスを少なくとも1つ持つNetScalerクラスターの更新されたリストを取得するには、**Rediscover**オプションを使用します。

あるSDXアプライアンス上に存在するNetScalerインスタンスを、別のSDXアプライアンス上に構成されたクラスターに追加する

1. NetScalerインスタンスを追加したいSDXアプライアンスにログオンします。
2. **Configuration**タブで、**NetScaler**に移動し、**Clusters**をクリックします。
3. **Add Node**をクリックします。
4. **Add Node**ダイアログボックスで、クラスターノードの追加に必要なパラメータを設定します。パラメータの説明については、対応するフィールドにマウスポインターを合わせます。注: 次のパラメータの値が、クラスターIPアドレスとクラスターIPパスワードのパラメータが、ノードを追加するクラスターのものであることを確認してください。
5. **Next**をクリックして、構成の概要を表示します。
6. **Finish**をクリックして、ノードをクラスターに追加します。

クラスターリンクアグリゲーションの構成

クラスターリンクアグリゲーションは、その名の通り、クラスターノードインターフェイスのグループをチャンネルに結合します。これはNetScalerのリンクアグリゲーション (LA) の拡張機能です。唯一の違いは、リンクアグリゲーションではインターフェイスが同じデバイス上にある必要があるのに対し、クラスターリンクアグリゲーションではインターフェイスがクラスターの異なるノード上にあることです。リンクアグリゲーションの詳細については、「[リンクアグリゲーションの構成](#)」を参照してください。

たとえば、2つのSDXアプライアンスにまたがる6ノードクラスターを考えます。このクラスターでは、6つのノードすべてがアップストリームスイッチに接続されています。インターフェイス 0/1/2、1/1/3、2/1/4、3/1/2、4/1/3、および5/1/4をバインドすることで、クラスターLAチャンネル (CLA/1) が形成されます。



クラスターLAチャンネルには、次の属性があります。

- 各チャンネルには、クラスターノード間で合意された一意のMACアドレスがあります。
- チャンネルは、ローカルおよびリモートのSDXノードのインターフェイスの両方をバインドできます。
- クラスターでは、最大4つのクラスターLAチャンネルがサポートされます。
- 各クラスターLAチャンネルには、最大16個のインターフェイスをバインドできます。
- バックプレーンインターフェイスは、クラスターLAチャンネルの一部にすることはできません。

- インターフェイスがクラスターLAチャンネルにバインドされている場合、チャンネルパラメーターがネットワークインターフェイスパラメーターよりも優先されます。
- ネットワークインターフェイスは、1つのチャンネルにのみバインドできます。
- クラスターLAチャンネル (CLA/1など) またはそのメンバーインターフェイスで、クラスターノードへの管理アクセスを構成しないでください。ノードがINACTIVEの場合、対応するクラスターLAインターフェイスはPOWER OFFとマークされ、管理アクセスが失われます。



クラスターIPアドレスと外部接続デバイスで同様の構成を実装します。可能であれば、MACアドレスではなくIPアドレスまたはポートに基づいてトラフィックを分散するようにアップストリームスイッチを構成してください。

留意点:

- LACPを有効にします（LACPモードをACTIVEまたはPASSIVEのいずれかに指定します）。
注: NetScalerクラスターと外部接続デバイスの両方でLACPモードがPASSIVEに設定されていないことを確認してください。
- クラスターLAチャンネルを作成する場合、LACPキーは5から8までの値を持つことができます。これらのLACPキーは、CLA/1、CLA/2、CLA/3、およびCLA/4にマッピングされます。
- SDXアプライアンスでは、クラスターリンクアグリゲーショングループ（CLAG）メンバーインターフェイスを他の仮想マシンと共有することはできません。
- アップストリームスイッチで、クラスターノードでの長時間のトラフィックブラックホールを避けるために、LACPタイムアウトを「short」に設定します。この設定は、LACPタイムアウトが経過するまで、アップストリームスイッチがCLAGとそのメンバーインターフェイスの電源オフを通知されない場合に役立ちます。

前提条件:

NetScalerインスタンスのクラスターを作成します。クラスターのノードは、同じSDXアプライアンス上、または同じサブネットで利用可能な他のSDXアプライアンス上のNetScalerインスタンスであることができます。

Management Serviceを使用してクラスターLAチャンネルを構成するには:

1. SDXアプライアンスにログオンします。
2. **Configuration**タブで、**NetScaler**に移動し、**Clusters**をクリックします。
3. **Cluster Instances**ページで、クラスターを選択し、**CLAG**をクリックします。



4. **Create CLAG** ダイアログボックスで、次の操作を行います。

- a. **Channel ID** ドロップダウンリストで、クラスターLAチャンネルIDを選択します。
- b. **Interfaces** セクションの**Available** 選択ボックスから、インターフェイスを選択し、**+**をクリックします。
- c. 選択されたインターフェイスは、「**Configured**」選択ボックスの下に表示されます。

5. 「**Setting**」セクションで、次の操作を行います。

- a. 「**Alias**」フィールドに、クラスターLAチャンネルの代替名を入力します。
- b. 「**LACP Timeout**」フィールドで、リンクがLACPDUを受信しない場合に、リンクが集約されなくなるまでの間隔を定義するために、次のいずれかの値を選択します。

SDXアプライアンスとパートナーノード上のリンクアグリゲーションに参加しているすべてのポートで、値が一致している必要があります。

- 「**Long**」 – 30秒
 - 「**Short**」 – 1秒
- c. 高可用性 (HA) 構成の場合、「**HA Monitoring**」チェックボックスをオンにして、チャンネルの障害イベントを監視します。HA MONが有効になっているLAチャンネルの障害は、HAフェイルオーバーをトリガーします。
 - d. 「**Tag All**」を選択して、このチャンネルで送信されるすべてのパケットに4バイトの802.1q タグを追加します。「**ON**」設定は、このチャンネルにバインドされているすべてのVLANにタグを適用します。「**OFF**」は、ネイティブVLAN以外のすべてのVLANにタグを適用します。

6. 「**Create**」をクリックして、いずれかのSDXアプライアンスのCLAGを構成します。

CLAGを作成する(/en-us/sdx/media/create-clag.png)

7. 「**Confirm**」ダイアログボックスで、「**Yes**」をクリックして、他のSDXアプライアンスのCLAG設定を更新します。

「

注:

- 「No」を選択した場合、CLAGは構成されません。
- 他のSDXアプライアンスのCLAG設定を手動で更新します。
- MTU設定は、両方のSDXアプライアンスで同じである必要があります。MTU設定は、いずれかのSDXアプライアンスで手動で変更する必要があります。

8. **CLAGs**ダイアログボックスでMTU設定を変更するには、次の操作を行います。
 - a. **CLA/1**を選択し、**編集**をクリックします。
 - b. **CLAGの構成**ダイアログボックスで、**MTU**フィールドにMTUを手動で設定し、**OK**をクリックします。
9. **確認**ダイアログボックスで、**はい**をクリックします。

Management Serviceに安全にアクセスするためのSSL暗号の構成

NetScaler SDXアプライアンスでサポートされているSSL暗号のリストから、SSL暗号スイートを選択できます。SSL暗号の任意の組み合わせをバインドして、HTTPS経由でSDX Management Serviceに安全にアクセスできます。SDXアプライアンスは、類似の暗号の組み合わせである37の定義済み暗号グループを提供しており、サポートされているSSL暗号のリストからカスタム暗号グループを作成できます。

制限事項

- キー交換が「DH」または「ECC-DHE」の暗号のバインドはサポートされていません。
- 認証が「DSS」の暗号のバインドはサポートされていません。
- サポートされているSSL暗号リストに含まれていない暗号のバインド、またはこれらの暗号をカスタム暗号グループに含めることはサポートされていません。

サポートされているSSL暗号

次の表に、サポートされているSSL暗号を示します。「**プロトコル**」列の値は、サポートされている最も低いプロトコルです。たとえば、SSLv3がリストされている場合、SSLv3/TLSv1/TLSv1.1/TLSv1.2はすべてサポートされます。

CITRIX暗号名	OPENSSL暗号名	16進コード	プロトコル	キー交換アルゴリズム	認証アルゴリズム	メッセージ認証コード (MAC) アルゴリズム
TLS1-AES-256-CBC-SHA	AES256-SHA	0x0035	エスエスエルブイスリー	RSA	RSA	AES(256)
TLS1-AES-128-CBC-SHA	AES128-SHA	0x002F	エスエスエルブイスリー	RSA	RSA	AES(128)
TLS1.2-AES-256-SHA256	AES256-SHA256	0x003D	TLSv1.2	RSA	RSA	AES(256)
TLS1.2-AES-128-SHA256	AES128-SHA256	0x003C	TLSv1.2	RSA	RSA	AES(128)
TLS1.2-AES256-GCM-SHA384	AES256-GCM-SHA384	0x009D	TLSv1.2	RSA	RSA	AES-GCM(256)
TLS1.2-AES128-GCM-SHA256	AES128-GCM-SHA256	0x009C	TLSv1.2	RSA	RSA	AES-GCM(128)
TLS1-ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA	0xC014	エスエスエルブイスリー	ECC-DHE	RSA	AES(256)

CITRIX暗号名	OPENSSL暗号名	16進コード	プロトコル	キー交換アルゴリズム	認証アルゴリズム	メッセージ認証コード (MAC) アルゴリズム
TLS1-ECDHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA	0xC013	エスエスエルブリースリー	ECC-DHE	RSA	AES(128)
TLS1.2-ECDHE-RSA-AES-256-SHA384	ECDHE-RSA-AES256-SHA384	0xC028	TLSv1.2	ECC-DHE	RSA	AES(256)
TLS1.2-ECDHE-RSA-AES-128-SHA256	ECDHE-RSA-AES128-SHA256	0xC027	TLSv1.2	ECC-DHE	RSA	AES(128)
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA-AES256-GCM-SHA384	0xC030	TLSv1.2	ECC-DHE	RSA	AES-GCM(256)
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA-AES128-GCM-SHA256	0xC02F	TLSv1.2	ECC-DHE	RSA	AES-GCM(128)
TLS1.2-DHE-RSA-AES-256-SHA256	DHE-RSA-AES256-SHA256	0x006B	TLSv1.2	DH	RSA	AES(256)

CITRIX暗 号名	OPENSSL暗号名	16進コード	プロトコル	キー交換アル ゴリズム	認証アルゴ リズム	メッセージ 認証コード (MAC) ア ルゴリズム
TLS1.2- DHE- RSA- AES-128- SHA256	DHE- RSA- AES128- SHA256	0x0067	TLSv1.2	DH	RSA	AES(128)
TLS1.2- DHE- RSA- AES256- GCM- SHA384	DHE- RSA- AES256- GCM- SHA384	0x009F	TLSv1.2	DH	RSA	AES- GCM(256)
TLS1.2- DHE- RSA- AES128- GCM- SHA256	DHE- RSA- AES128- GCM- SHA256	0x009E	TLSv1.2	DH	RSA	AES- GCM(128)
TLS1- DHE- RSA- AES-256- CBC-SHA	DHE- RSA- AES256- SHA	0x0039	エスエス エルv3	DH	RSA	AES(256)
TLS1- DHE- RSA- AES-128- CBC-SHA	DHE- RSA- AES128- SHA	0x0033	エスエス エルv3	DH	RSA	AES(128)
TLS1- DHE- DSS- AES-256- CBC-SHA	DHE- DSS- AES256- SHA	0x0038	エスエス エルブイ スリー	DH	DSS	AES(256)

CITRIX暗号名	OPENSSL暗号名	16進コード	プロトコル	キー交換アルゴリズム	認証アルゴリズム	メッセージ認証コード (MAC) アルゴリズム
TLS1-DHE-DSS-AES-128-CBC-SHA	DHE-DSS-AES128-SHA	0x0032	エスエスエルブイスリー	DH	DSS	AES(128)
TLS1-ECDHE-RSA-DES-CBC3-SHA	ECDHE-RSA-DES-CBC3-SHA	0xC012	エスエスエルブイスリー	ECC-DHE	RSA	3DES(168)
SSL3-EDH-RSA-DES-CBC3-SHA	EDH-RSA-DES-CBC3-SHA	0x0016	エスエスエルブイスリー	DH	RSA	3DES(168)
SSL3-EDH-DSS-DES-CBC3-SHA	EDH-DSS-DES-CBC3-SHA	0x0013	エスエスエルブイスリー	DH	DSS	3DES(168)
TLS1-ECDHE-RSA-RC4-SHA	ECDHE-RSA-RC4-SHA	0xC011	エスエスエルブイスリー	ECC-DHE	RSA	RC4(128)
SSL3-DES-CBC3-SHA	DES-CBC3-SHA	0x000A	エスエスエルブイスリー	RSA	RSA	3DES(168)

CITRIX暗号名	OPENSSL暗号名	16進コード	プロトコル	キー交換アルゴリズム	認証アルゴリズム	メッセージ認証コード (MAC) アルゴリズム
SSL3-RC4-SHA	RC4-SHA	0x0005	エスエスエルブイスリー	RSA	RSA	RC4(128)
SSL3-RC4-MD5	RC4-MD5	0x0004	エスエスエルブイスリー	RSA	RSA	RC4(128)
SSL3-DES-CBC-SHA	DES-CBC-SHA	0x0009	エスエスエルブイスリー	RSA	RSA	DES(56)
SSL3-EXP-RC4-MD5	EXP-RC4-MD5	0x0003	エスエスエルブイスリー	RSA(512)	RSA	RC4(40)
SSL3-EXP-DES-CBC-SHA	EXP-DES-CBC-SHA	0x0008	SSLv3 プロトコル	RSA(512)	RSA	DES(40)
SSL3-EXP-RC2-CBC-MD5	EXP-RC2-CBC-MD5	0x0006	SSLv3 プロトコル	RSA(512)	RSA	RC2(40)
SSL2-DES-CBC-MD5	DHE-DSS-AES128-SHA256	0x0040	エスエスエルブイツー	RSA	RSA	DES(56)
SSL3-EDH-DSS-DES-CBC-SHA	EDH-DSS-DES-CBC-SHA	0x0012	エスエスエルブイスリー	DH	DSS	DES(56)

CITRIX暗 号名	OPENSSL暗号名	16進コード	プロトコル	キー交換アル ゴリズム	認証アルゴ リズム	メッセージ 認証コード (MAC) ア ルゴリズム
SSL3- EXP- EDH- DSS- DES- CBC-SHA	EXP- EDH- DSS- DES- CBC-SHA	0x0011	SSLバー ジョン3	DH(512)	DSS	DES(40)
SSL3- EDH- RSA- DES- CBC-SHA	EDH- RSA- DES- CBC-SHA	0x0015	SSLバー ジョン3	DH	RSA	DES(56)
SSL3- EXP- EDH- RSA- DES- CBC-SHA	EXP- EDH- RSA- DES- CBC-SHA	0x0014	SSLv3 (エスエス エルブイ スリー)	DH(512)	RSA	DES(40)
SSL3- ADH- RC4-MD5	ADH- RC4-MD5	0x0018	SSLv3 (エスエス エルブイ スリー)	DH	なし	RC4(128)
SSL3- ADH- DES- CBC3- SHA	ADH- DES- CBC3- SHA	0x001B	エスエス エルブイ スリー	DH	なし	3DES(16 8)
SSL3- ADH- DES- CBC-SHA	ADH- DES- CBC-SHA	0x001A	エスエス エルブイ スリー	DH	なし	DES(56)
TLS1- ADH-	ADH- AES128- SHA	0x0034	SSLバー ジョン3	DH	なし	AES(128)

CITRIX暗号名	OPENSSL暗号名	16進コード	プロトコル	キー交換アルゴリズム	認証アルゴリズム	メッセージ認証コード (MAC) アルゴリズム
AES-128-CBC-SHA						
TLS1-ADH-AES-256-CBC-SHA	ADH-AES256-SHA	0x003A	SSLバージョン3	DH	なし	AES(256)
SSL3-EXP-ADH-RC4-MD5	EXP-ADH-RC4-MD5	0x0017	SSLバージョン3	DH(512)	なし	RC4(40)
SSL3-EXP-ADH-DES-CBC-SHA	EXP-ADH-DES-CBC-SHA	0x0019	SSLバージョン3	DH(512)	なし	DES(40)
SSL3-NULL-MD5	NULL-MD5	0x0001	エスエスエルv3	RSA	RSA	なし
SSL3-NULL-SHA	NULL-SHA	0x0002	エスエスエルv3	RSA	RSA	なし

事前定義された暗号グループ

次の表に、SDXアプライアンスによって提供される事前定義された暗号グループを示します。

暗号グループ名	説明
ALL	NULL暗号を除く、SDXアプライアンスでサポートされているすべての暗号
DEFAULT	暗号化強度 >= 128ビットのデフォルト暗号リスト

暗号グループ名	説明
kRSA	鍵交換アルゴリズムがRSAである暗号
KEDH	鍵交換アルゴリズムがEphemeral-DHである暗号
DH	鍵交換アルゴリズムがDHである暗号
EDH	キー交換/認証アルゴリズムがDHの暗号スイート
aRSA	認証アルゴリズムがRSAの暗号スイート
aDSS	認証アルゴリズムがDSSの暗号スイート
aNULL	認証アルゴリズムがNULLの暗号スイート
DSS	認証アルゴリズムがDSSの暗号スイート
DES	暗号化アルゴリズムがDESの暗号スイート
3DES	暗号化アルゴリズムが3DESの暗号スイート
RC4	暗号化アルゴリズムがRC4の暗号スイート
RC2	暗号化アルゴリズムがRC2である暗号
NULL	暗号化アルゴリズムがNULLである暗号
MD5	MACアルゴリズムがMD5である暗号
SHA1	MACアルゴリズムがSHA-1である暗号
SHA	MACアルゴリズムがSHAである暗号
NULL	暗号化アルゴリズムがNULLである暗号
RSA	鍵交換/認証アルゴリズムがRSAである暗号
ADH	鍵交換アルゴリズムがDHで、認証アルゴリズムがNULLの暗号スイート
エスエスエルバイツ	SSLv2プロトコルの暗号スイート

TLSv1	SSLv3/TLSv1 プロトコルの暗号スイート
TLSv1_ONLY	TLSv1 プロトコルの暗号スイート
EXP	エクスポート暗号スイート
EXPORT	エクスポート暗号スイート
EXPORT40	40ビット暗号化を使用したエクスポート暗号スイート
EXPORT56	56ビット暗号化のエクスポート暗号
低	低強度の暗号 (56ビット暗号化)
中	中強度の暗号 (128ビット暗号化)
高	高強度の暗号 (168ビット暗号化)
AES	AES暗号
FIPS	FIPS承認済み暗号
ECDHE	楕円曲線一時DH暗号
AES-GCM	EncアルゴリズムがAES-GCMの暗号
SHA2	MACアルゴリズムがSHA-2の暗号

事前定義された暗号グループを表示する

事前定義された暗号グループを表示するには、**構成**タブで、ナビゲーションペインの**管理サービス**を展開し、**暗号グループ**をクリックします。

カスタム暗号グループを作成する

サポートされているSSL暗号のリストから、カスタム暗号グループを作成できます。

カスタム暗号グループを作成するには:

1. **構成**タブで、ナビゲーションペインの**管理サービス**を展開し、**暗号グループ**をクリックします。
2. **暗号グループ**ペインで、**追加**をクリックします。

3. **暗号グループの作成**ダイアログボックスで、以下を実行します。
 - a. **グループ名**フィールドに、カスタム暗号グループの名前を入力します。
 - b. **暗号グループの説明**フィールドに、カスタム暗号グループの簡単な説明を入力します。
 - c. **暗号スイート**セクションで、**追加**をクリックし、サポートされているSSL暗号のリストに含める暗号を選択します。
 - d. **作成**をクリックします。

既存のSSL暗号バインディングを表示する

既存の暗号バインディングを表示するには、**Configuration**タブのナビゲーションペインで、**System**を展開し、**System Settings**の下にある**Configure SSL Settings**をクリックします。

SSL設定の構成(/en-us/sdx/media/configure-ssl-settings.png)

注:

Management Serviceの最新バージョンにアップグレードすると、既存の暗号スイートのリストにOpenSSL名が表示されます。アップグレードされたManagement Serviceから暗号をバインドすると、表示はCitrix®の命名規則を使用します。

暗号をHTTPSサービスにバインドする

1. **Configuration**タブのナビゲーションペインで、**System**をクリックします。
2. **System**ペインの**System Settings**の下にある**Configure SSL Settings**をクリックします。
3. **Edit Settings**ペインで、**Ciphers Suites**をクリックします。
4. **Ciphers Suites**ペインで、次のいずれかを実行します。
 - 定義済みの暗号グループから暗号グループを選択するには、**Cipher Groups**を選択し、**Cipher Groups**リストから暗号グループを選択して、**OK**をクリックします。
 - サポートされている暗号のリストから選択するには、**Cipher Suites**チェックボックスをオンにし、**Add**をクリックして暗号を選択し、**OK**をクリックします。

SDXアプライアンスの構成データのバックアップと復元

NetScaler SDXアプライアンスのバックアッププロセスは、以下の内容を含むバックアップファイルを作成する単一ステップのプロセスです。

- シングルバンドルイメージ:

- Citrix Hypervisor™ イメージ
- Citrix Hypervisor のホットフィックスと補足パック
- Management Service イメージ
- XVA イメージ
- アップグレードイメージ
- SDX構成
- 構成

バックアップフォルダは /var/mps/backup/ です。

現在の構成をバックアップする

1. **Configuration** タブのナビゲーションペインで、**Management Service** を展開し、**Backup Files** をクリックします。
2. **Backup Files** ペインで、**Back Up** をクリックします。
3. **New Backup File** ダイアログボックスで、バックアップファイルを暗号化するために、**Password Protect file** チェックボックスをオンにします。
4. 「**Password**」および「**Confirm Password**」フィールドに、バックアップファイルのパスワードを入力して確認します。
5. 「**Continue**」をクリックします。

バックアッププロセスによってバックアップファイルが作成されます。バックアップファイルのファイル名には、Management Service の現在の IP アドレスと、バックアップが取得されたときのタイムスタンプが含まれます。バックアップファイルに不整合がないか確認するには、SDX GUI から「**Configuration > System > Events/Alarms**」に移動します。

スケジュールされたバックアップ

デフォルトでは、SDX はバックアップポリシーを使用して24時間ごとにバックアップを作成します。バックアップポリシーを使用すると、SDX アプライアンスに保持するバックアップファイルの数を定義できます。また、スケジュールされたバックアップファイルをパスワードで暗号化して、バックアップファイルのセキュリティを確保することもできます。

バックアップポリシーを編集する

1. 「**Configuration**」タブで、「**System**」をクリックします。
2. 「**Policy Administration**」ペインで、「**Backup Policy**」をクリックします。

3. 「**Configure backup policy**」 ペインで、次の操作を実行します。
 - a. 「**Previous backups to retain**」 フィールドに、保持するバックアップファイルの数を入力します。
 - b. バックアップファイルを暗号化するには、「**Encrypt Backup File**」チェックボックスをオンにします。
 - c. 「**Password**」および「**Confirm Password**」フィールドに、バックアップファイルを暗号化するためのパスワードを入力して確認します。

バックアップファイルを外部バックアップサーバーに手動で転送する

バックアップファイルを手動で転送する前に、外部バックアップサーバーの詳細があることを確認してください。

バックアップファイルを外部バックアップサーバーに転送する

1. 「**Configuration**」 タブのナビゲーションペインで、「**Management Service**」を展開し、「**Backup Files**」をクリックします。
2. 「**Backup Files**」 ペインで、バックアップファイルを選択し、「**Transfer**」をクリックします。
3. 「**Server**」 フィールドに、外部バックアップサーバーのホスト名またはIPアドレスを入力します。
4. 「**User Name**」 フィールドと 「**Password**」 フィールドに、外部バックアップサーバーにアクセスするためのユーザー名とパスワードを入力します。
5. 「**Port**」 フィールドに、ポート番号を入力します。
6. 「**Transfer Protocol**」 フィールドで、バックアップファイルを外部バックアップサーバーに転送するために使用するプロトコルを選択します。
7. 「**Directory Path**」 フィールドに、バックアップファイルを保存する外部バックアップサーバー内のディレクトリのパスを入力します。
8. バックアップファイルを外部バックアップサーバーに転送した後、SDXアプライアンスからバックアップファイルを削除するには、「**Delete file from Management Service**」を選択します。
9. 「**OK**」 をクリックします。

アプライアンスを復元する

SDXアプライアンスを、バックアップファイルで利用可能な構成に復元できます。アプライアンスの復元中、現在のすべての構成が削除されます。

注意点:

- 別のSDXアプライアンスのバックアップファイルを使用してSDXアプライアンスを復元する前に、バックアップファイルで利用可能な設定に従ってManagement Serviceのネットワーク設定を追加します。
- バックアップが取得されたプラットフォームバリエーションが、復元しようとしているプラットフォームバリエーションと同じであることを確認してください。2つの異なるプラットフォームバリエーション間でバックアップファイルを復元することはサポートされていません。
- Citrix®は、ネットワーク構成が設定された後にのみSDXバックアップを復元することを推奨します。SVMには以下のネットワーク設定を指定できます。
 - SVM IP アドレス
 - ハイパーバイザー IP アドレス
 - サブネットマスク
 - ゲートウェイ
 - DNS サーバー

バックアップファイルからアプライアンスを復元する

1. 「**Configuration**」タブのナビゲーションペインで、「**Management Service**」を展開し、「**Backup Files**」をクリックします。
2. 「**Backup Files**」ペインで、バックアップファイルをクリックし、「**OK**」をクリックします。
3. 「**Restore**」ダイアログボックスで、「**Appliance Restore**」を選択し、「**Proceed**」をクリックします。

アプリケーション復元のさまざまなコンポーネントが表示されます。

- ライセンス
- SDX イメージ
- XVA ファイル
- NetScaler の構成
- 概要

バックアップファイルに必要なコンポーネントが不足している場合は、続行する前に不足している要素をアップロードするように求められます。

バックアップファイルを現在のSDXシングルバンドルイメージバージョンに復元できるかどうかについては、次の表を参照してください。シングルバンドルイメージの経験則として、下位バージョンのバックアップを上位バージョンに復元することはできません。

現在のSDXシングルバンドルイメージバージョン	バックアップファイルバージョン
11.1	11.1、12.0、12.1、13.0はサポートされています。11.0はサポートされていません。
12.0	12.0、12.1、13.0はサポートされています。11.0および11.1はサポートされていません。
12.1	12.1、13.0はサポートされています。11.0、11.1、12.0はサポートされていません。
13.0	13.0はサポートされています。11.0、11.1、12.0、12.1はサポートされていません。
13.1	13.1はサポートされています。11.0、11.1、12.0、12.1、13.0はサポートされていません。

4. **License** ページで、有効なライセンスが存在することを確認し、**Next** をクリックします。
5. 「**SDX Image**」ページが表示されます。リストアの実行にSDXイメージが不要な場合は、「**Next**」をクリックします。それ以外の場合は、プロンプトが表示されたら有効なSDXイメージをアップロードし、「**Next**」をクリックします。
6. 「**XVA File**」ページが開きます。すべてのインスタンスのXVAイメージが存在する場合は、「**Next**」をクリックします。バックアップファイルにいずれかのインスタンスのXVAファイルがない場合は、アップロードするか、そのインスタンスのリストアをスキップできます。「**Next**」をクリックして次のページに進みます。
7. NetScaler Configurationページが開きます。NetScaler構成ファイルは必須ではありません。構成をリストアせずにインスタンスをプロビジョニングできます。バックアップファイルにNetScaler構成ファイルがない場合は、インスタンスのプロビジョニングのみを進めるか、インスタンスのリストアをスキップできます。「**Next**」をクリックして次のページに進みます。
8. バックアップファイルに存在するすべてのインスタンスに関する以下の詳細情報が記載された概要ページが表示されます。
 - IPアドレス
 - ホスト名

- SDXバージョン
- XVAバージョン
- バージョンビット
- リストア: アプライアンスまたはインスタンスがリストアの準備ができている場合は、チェックマークが表示されます。そうでない場合は、バツ印が表示されます。
- エラーメッセージ: アプライアンスまたはインスタンスがリストアの準備ができていない場合は、その理由を説明するエラーメッセージが表示されます。

9. 「**Restore**」をクリックして、アプリケーションのリストアプロセスを完了します。

NetScalerインスタンスをリストアする

SDXアプライアンスのNetScalerインスタンスを、バックアップファイルで利用可能なNetScalerインスタンスにリストアできます。

NetScalerインスタンスのバックアップファイルの「**Gateway**」フィールドに値がない場合、リストア操作は次のいずれかの条件が満たされている場合にのみ許可されます。

- Management Service と NetScaler インスタンスの IP アドレスは、同じサブネット上にある必要があります。
- **内部ネットワーク経由で管理**を有効にする必要があります。

これらの条件が満たされていない場合、Management Service は強制的に**内部ネットワーク経由で管理**を有効にし、操作完了後に無効にします。**内部ネットワーク経由で管理**を有効にすることで、インスタンスが到達可能になり、復元が成功します。

注意点: VPX インスタンスは、次の場合に復元に失敗します。

- インスタンスに管理 NIC が割り当てられていない場合、および
- インスタンスが SDX Management Service から LACP 経由でのみ管理されている場合。SDX Management Service はチャンネル構成を自動的に復元できないため、復元は失敗します。この問題を回避するには、VPX インスタンスの復元を完了するために、チャンネル構成を手動で復元してください。

バックアップファイル内の NetScaler インスタンスを復元するには：

1. **構成**タブのナビゲーションペインで、**Management Service**を展開し、バックアップファイルをクリックします。
2. **バックアップファイル**ペインで、バックアップファイルを選択し、**復元**をクリックします。
3. **復元**ダイアログボックスで、**インスタンスの復元**を選択します。

4. 復元する NetScaler インスタンスを選択し、**続行**をクリックします。
5. (オプション) バックアップファイルが暗号化されている場合、プロンプトが表示されたらパスワードを入力し、**OK**をクリックします。

注：

復元されるインスタンスを実行する SDX アプライアンスに、適切な XVA、ビルドイメージ、およびチャネル構成が存在することを確認してください。

アプライアンスのリセットを実行する

NetScaler SDXアプライアンスでは、次のことができます。

- アプライアンスの構成をリセットします。

注:

構成をリセットするときは、アプライアンスのシリアル番号をパスワードとして使用してログオンする必要があります。

- アプライアンスを工場出荷時のバージョンにリセットします。
- アプライアンスを特定のシングルバンドルイメージバージョンにリセットします。

アプライアンスのリセットを実行する前に、アプライアンスにプロビジョニングされているすべての NetScaler インスタンスの設定を含め、アプライアンスに保存されているすべてのデータをバックアップしてください。

Citrix®は、ファイルをアプライアンスの外部に保存することをお勧めします。アプライアンスのリセットを実行すると、Management Serviceとの現在のクライアントセッションがすべて終了します。追加の構成タスクを行うには、Management Serviceに再度ログオンしてください。データを復元する準備ができたなら、Management Serviceを使用してバックアップファイルをインポートします。

Management Serviceは、アプライアンスをリセットするための次のオプションを提供します。

- 構成のリセット
- ファクトリーリセット
- クリーンインストール

アプライアンスの構成をリセットする

Management Serviceは、アプライアンスの構成をリセットするための構成リセットオプションを提供します。構成リセットオプションは、次の処理を実行します。

- VPXインスタンスを削除します。
- SSL証明書およびキーファイルを削除します。
- ライセンスおよびテクニカルアーカイブファイルを削除します。
- アプライアンス上のNTP構成を削除します。
- タイムゾーンをUTCに復元します。
- プルーニングおよびバックアップポリシーをデフォルト設定に復元します。
- Management Serviceイメージを削除します。
- NetScaler SDXイメージを削除します。
- アプライアンスで最後にアクセスされたイメージファイルを除く、すべてのXVAイメージを削除します。
- デフォルトのインターフェイス設定を復元します。
- デフォルトプロファイル、ユーザー、システム設定を含む、アプライアンスのデフォルト構成を復元します。
- Citrix Hypervisor™およびManagement Serviceのデフォルトパスワードを復元します。
- Management Serviceを再起動します。

アプライアンスの構成をリセット

1. **コンフィギュレーション > システム > システム管理グループ**に移動します。
2. 「**Appliance Reset**」をクリックします。
3. 「**Appliance Reset**」ダイアログボックスで、「**Reset Type**」リストから「**Config Reset**」を選択します。
4. 「**OK**」をクリックします。

アプライアンスを工場出荷時のバージョンにリセットする

Management Service には、アプライアンスを工場出荷時のバージョンにリセットする Factory Reset オプションが用意されています。Factory Reset オプションは、Management Service および Citrix Hypervisor の現在の IP アドレスを、Management Service および Citrix Hypervisor のデフォルト IP アドレスにリセットします。

アプライアンスに保存されているすべてのデータ (アプライアンスにプロビジョニングされているすべての NetScaler インスタンスの設定を含む) をバックアップしてください。Citrix では、ファイルをアプライアンスの外部に保存することをお勧めします。工場出荷時の状態にリセットすると、Management Service との現在のクライアントセッションはすべて終了します。追加の構成タスクを行うには、Management Service に再度ログオンしてください。データを復元する準備ができたなら、Management Service を使用してバックアップファイルをインポートします。

重要

工場出荷時の状態にリセットする前に、シリアルコンソールケーブルをアプライアンスに接続してください。

アプライアンスを工場出荷時のバージョンにリセットする

1. **設定 > システム > システム管理** に移動します。
2. 「**Appliance Reset**」をクリックします。
3. 「**Appliance Reset**」ダイアログボックスで、「**Reset Type**」リストから「**Factory Reset**」を選択します。
4. 「**OK**」をクリックします。

アプライアンスをシングルバンドルイメージバージョンにリセットする

Management Service には、アプライアンスに任意のバージョンのシングルバンドルイメージをインストールできる Clean Install オプションが用意されています。これにより、シングルバンドルイメージを新しいデフォルトのブートイメージとして新規インストールできます。クリーンインストールでは、SDX アプライアンスのネットワーク設定を除く既存の構成が削除されます。

注:

SDXアプライアンスがソフトウェアバージョン11.0以前で出荷された場合、バージョン13.1以降へのクリーンインストールは失敗します。

クリーンインストールオプションは以下でサポートされています。

シングルバンドルイメージバージョン	SDXプラットフォーム
11.0.xx	SDX 14xxx、SDX 25xxx。注: 10Gのファクトリパーティションがある場合、他のSDXブ

シングルバンドルイメージバージョン	SDXプラットフォーム
	プラットフォームでもクリーンインストールオプションがサポートされます。
11.1.xx	SDX 14xxx、SDX 25xxx。注: 10Gのファクトリパーティションがある場合、他のSDXプラットフォームでもクリーンインストールオプションがサポートされます。
11.1.51.x	すべてのSDXプラットフォーム。
12.1.xx	すべてのSDXプラットフォーム。
13.0.xx	すべてのSDXプラットフォーム。
13.1.xx	すべてのSDXプラットフォーム。

前提条件

以下を確認してください。

- すべてのプライマリ高可用性ノードを別のSDXアプライアンスにフェイルオーバーします。高可用性機能がない場合は、それに応じてダウンタイムを計画してください。
- シングルバンドルイメージをローカルマシンにダウンロードします。

重要:

クリーンインストールオプションを使用している間は、アプライアンスを再起動したり、電源を入れ直したりしないでください。アプライアンスは複数回再起動されます。

アプライアンスを単一のバンドルイメージバージョンにリセットする

1. **Configuration > System > System Administration** グループに移動します。
2. **Appliance Reset** をクリックします。
3. **Appliance Reset** ダイアログボックスで、**Reset Type** リストから **Clean Install** を選択します。
4. **OK** をクリックします。

外部認証サーバーのカスケーディング

複数の外部認証サーバーをカスケード接続することで、外部ユーザーの認証と承認のための継続的で信頼性の高いプロセスが提供されます。最初の認証サーバーで認証が失敗した場合、管理サービスは2番目の外部認証サーバーを使用してユーザーを認証しようとします。

カスケード認証を有効にするには、外部認証サーバーを管理サービスに追加します。詳細については、「[外部認証の構成](#)」を参照してください。サポートされている外部認証サーバー（RADIUS、LDAP、TACACS）の任意のタイプを追加できます。たとえば、カスケード認証用に4つの外部認証サーバーを追加するには、RADIUS、LDAP、TACACSサーバーの任意の組み合わせを追加できます。また、同じタイプのサーバーを4つすべて追加することもできます。NetScaler Consoleでは、最大32台の外部認証サーバーを設定できます。

注：

CLIを介した外部認証サーバーのカスケーディングはサポートされていません。

外部認証サーバーをカスケード接続する

1. **構成**タブで、**システム**の下にある**認証**を展開します。
2. **認証**ページで、**認証構成**をクリックします。
3. **認証構成**ページで、**サーバータイプ**ドロップダウンリストから**EXTERNAL**を選択します（外部サーバーのみをカスケードできます）。
4. **挿入**をクリックし、開いた**外部サーバー**ページで、カスケードする認証サーバーを1つまたは複数選択します。
5. **OK**をクリックします。

選択したサーバーは、次の図に示すように**認証サーバー**ページに表示されます。認証の順序を変更するには、サーバー名の横にあるアイコンを使用して、リスト内でサーバーを上下に移動します。



ユーザーのロックを解除する

NetScaler SDX管理者は、ロックアウト間隔が期限切れになる前にユーザーのロックを解除できます。ユーザーがコンソール経由でManagement Serviceにログインする場合、ロックアウトは適用されません。ロックアウト間隔も秒から分に変更されます。最小値 = 1分。最大値 = 30分。

GUIを使用してユーザーのロックを解除する

1. 設定 > システム > ユーザー管理 > ユーザー に移動します。
2. ロックを解除するユーザーを選択します。
3. **Unlock** をクリックします。

CLIを使用してユーザーのロックを解除する

コマンドプロンプトで、次のように入力します。

```
set systemuser id=<ID> unlock=true
```

アドミンプロファイルでnsroot以外のユーザーを作成する

nsrootユーザーは、NetScalerにおける最高レベルのアクセスと制御を持つデフォルトの管理者アカウントです。nsrootユーザーは、システム設定の変更、ネットワーク構成、ライセンス管理、セキュリティポリシーの設定、ログへのアクセスなど、システム内であらゆる操作を実行できます。

NetScalerリリース14.1-43x以降、NetScaler SDX Management Serviceを使用して、アドミンプロファイルでnsroot以外のユーザーを作成および管理できます。nsroot以外のユーザーは、アクセスが制限されたアカウントです。管理者は、システム内で実行する必要がある操作に基づいて、事前定義された権限を持つロールをnsroot以外のユーザーに割り当てます。ユーザーには、トラフィックの監視や構成の管理など、特定の権限を付与できますが、完全な管理者権限は付与されません。

この機能強化により、nsroot以外のユーザーが特定の管理タスクを実行できるようになることで、管理タスクの処理に柔軟性がもたらされます。これにより、アドミンプロファイルの管理が改善され、頻繁なパスワード変更の必要性が減り、全体的なユーザー管理エクスペリエンスが向上します。

SDXでアドミンプロファイル内のnsroot以外のユーザーを使用できるようにする

次の手順は、アドミンプロファイルでnsroot以外のユーザーを管理するための主要な手順をまとめたものです。

1. NetScaler SDXにログオンします。
2. nsroot以外のユーザー名でアドミンプロファイルを作成します。
3. NetScalerインスタンスを作成し、nsrootアドミンプロファイルを割り当てます。

注:

NetScalerインスタンスの作成は、nsrootユーザープロファイルでのみ許可されます。

4. NetScalerインスタンスを編集し、nsroot以外の管理者プロファイルを割り当てます。
5. 前のステップで作成したNetScalerインスタンスに、nsrootユーザーを使用してログインします。
6. 必要な権限を割り当てるために、システムコマンドポリシーをバインドします。
7. 構成を保存します。

非nsrootユーザーで管理者プロファイルを作成する

1. **NetScaler® > Admin Profiles** に移動します。
2. **追加** をクリックして、**NetScaler プロファイルの作成** ページを開きます。
3. **ユーザー名** フィールドに、非nsroot名を入力します。
4. 必要に応じて他のフィールドを更新し、**作成** をクリックします。



管理サービスを使用してNetScalerインスタンスを作成する

1. **NetScaler > インスタンス** に移動します。
2. **追加** をクリックして、**NetScaler のプロビジョニング** ページを開きます。
3. nsroot管理者プロファイルを割り当てます。
4. 必須フィールドに入力し、**完了** をクリックします。



NetScalerインスタンスを編集して、非nsroot管理者プロファイルを割り当てる

1. **NetScaler > インスタンス** に移動します。
2. NetScalerインスタンスを選択し、**編集** をクリックして、**NetScaler の構成** ページを開きます。
3. すでに作成した非nsroot管理者プロファイルを割り当てます。
4. 必須フィールドに入力し、**完了** をクリックします。

NetScalerインスタンスを編集(/en-us/sdx/media/non-nsroot-edit-ns-instance.png)

NetScalerインスタンスにシステムコマンドポリシーをバインドする

1. 管理サービスを介して作成したNetScalerインスタンスにログインします。
2. **System > User Administration > Users**に移動します。
3. **追加**をクリックして、**システムユーザー**ページを開きます。

システムユーザーを追加(/en-us/sdx/media/non-nsroot-system-user.png)

4. 必要な詳細を入力し、**続行**をクリックします。
5. システムユーザーページで、**Bindings > System Command Policy**に移動します。
6. **ユーザーコマンドポリシーバインディング**ウィンドウで、目的のポリシーを選択し、**バインド**をクリックします。ポリシーをバインド(/en-us/sdx/media/non-nsroot-bind-policy.png)
7. ポリシーをバインドした後、**保存**をクリックします。

NetScalerインスタンスで非nsrootユーザーを使用するためのガイドライン

- NetScalerインスタンスは、nsrootユーザープロファイルを使用してのみ作成できます。
- 非nsrootプロファイルは、NetScalerインスタンスの作成中ではなく、編集中にのみ割り当てることができます。
- 非nsrootプロファイルにコマンドポリシーを割り当てない場合、NetScalerインスタンスは「サービス停止」状態になります。適切なコマンドポリシーを割り当てて復元してください。
- システムコマンドポリシーが **superuser** に設定されている場合、非nsrootプロファイルを切り替えることができます。そうでない場合、切り替えはできません。プロファイルは常にnsrootユーザープロファイルに切り替えることができます。

NetScalerインスタンスのプロビジョニング

注：

NetScaler SDXアプライアンスをリリース13.1にインストールまたはアップグレードすると、Console Advisory Connectはデフォルトで有効になります。詳細については、「データガバナンスとConsole Advisory Connect」を参照してください。

Management Serviceを使用して、SDXアプライアンスに1つ以上のNetScalerインスタンスをプロビジョニングできます。インストールできるインスタンスの数は、購入したライセンスによって異なります。追加されたインスタンスの数がライセンスで指定された数と等しい場合、Management Serviceはそれ以上のNetScalerインスタンスのプロビジョニングを許可しません。

注：

基盤となるハードウェアプラットフォームに関係なく、1つのネットワークインターフェイスに最大20個のVPXインスタンスを設定できます。

SDXアプライアンスにNetScaler VPXインスタンスをプロビジョニングするには、次の手順を実行します。

1. NetScalerインスタンスにアタッチする管理者プロファイルを定義します。このプロファイルは、Management ServiceがADCインスタンスをプロビジョニングし、後でインスタンスと通信して構成データを取得するために使用するユーザー資格情報を指定します。デフォルトの管理者プロファイルを使用することもできます。
2. .xvaイメージファイルをManagement Serviceにアップロードします。
3. Management ServiceのNetScalerプロビジョニングウィザードを使用してNetScalerインスタンスを追加します。Management Serviceは、NetScalerインスタンスをSDXアプライアンスに自動的に展開し、インスタンスの構成詳細をダウンロードします。

警告

インスタンスのプロビジョニングされたネットワークインターフェイスまたはVLANを変更する場合は、インスタンスで直接変更するのではなく、Management Serviceを使用してください。

管理者プロファイルの作成

管理者プロファイルは、Management ServiceがNetScalerインスタンスをプロビジョニングする際に使用するユーザー資格情報を指定します。これらの資格情報は、後でインスタンスと通信して構成データを取得する際に使用されます。管理者プロファイルで指定されたユーザー資格情報は、クライアントがCLIまたはGUIを介してNetScalerインスタンスにログオンする際にも使用されます。

管理者プロファイルを使用すると、Management ServiceとVPXインスタンスがセキュアチャネル経由またはHTTPを使用してのみ相互に通信するように指定することもできます。

インスタンスのデフォルトの管理者プロファイルは、デフォルトの管理者ユーザー名を指定します。このプロファイルは変更または削除できません。ただし、インスタンスをプロビジョニングするときに、ユーザー定義の管理者プロファイルを作成してインスタンスにアタッチすることにより、デフォルトプロファイルを上書きする必要があります。Management Service管理者は、どのNetScalerインスタンスにもアタッチされていないユーザー定義の管理者プロファイルを削除できます。

重要

VPXインスタンスで直接パスワードを変更しないでください。そうすると、インスタンスはManagement Serviceから到達不能になります。パスワードを変更するには、まず管理者プロファイルを作成し、次にNetScalerインスタンスを変更して、管理者プロファイルリストからこのプロファイルを選択します。

高可用性セットアップでNetScalerインスタンスのパスワードを変更するには、まずセカンダリノードとして指定されたインスタンスのパスワードを変更します。次に、プライマリノードとして指定されたインスタンスのパスワードを変更します。パスワードはManagement Serviceを使用してのみ変更するようにしてください。

管理者プロファイルの作成

1. **Configuration** タブのナビゲーションペインで、**NetScaler Configuration** を展開し、**Admin Profiles** をクリックします。
2. **Admin Profiles** ペインで、**Add** をクリックします。
3. **Create Admin Profile** ダイアログボックスが表示されます。



次のパラメーターを設定します。

- プロファイル名: 管理者プロファイルの名前。デフォルトのプロファイル名は **nsroot** です。ユーザー定義のプロファイル名を作成できます。
 - パスワード: NetScaler インスタンスにログオンするために使用するパスワード。最大長: 31 文字。
 - SSHポート: SSHポートを設定します。デフォルトのポートは22です。
 - **NetScaler通信にグローバル設定を使用:** Management Service と NetScaler インスタンス間の通信設定をシステム設定で定義する場合は、これを選択します。このチェックボックスをオフにして、プロトコルをHTTPまたはHTTPSに変更できます。
 - Management Service と NetScaler インスタンス間の通信にHTTPプロトコルを使用するには、**http** オプションを選択します。
 - 「**https**」 オプションを選択して、Management Service と NetScaler インスタンス間の通信にセキュアチャネルを使用します。
- 4). **SNMP** で、バージョンを選択します。v2 を選択した場合は、手順 5 に進みます。v3 を選択した場合は、手順 6 に進みます。
 - 5). SNMP v2 で、**SNMP Community** 名を追加します。
 - 6). SNMP v3 で、**Security Name** と **Security Level** を追加します。
 - 7). **Timeout Settings** で、値を指定します。
 - 8). **Create** をクリックし、次に **Close** をクリックします。作成した管理者プロファイルが **Admin Profiles** ペインに表示されます。

Default 列の値が true の場合、デフォルトプロファイルが管理者プロファイルです。値が false の場合、ユーザー定義プロファイルが管理者プロファイルです。

ユーザー定義の管理者プロファイルを使用しない場合は、Management Service から削除できません。ユーザー定義の管理者プロファイルを削除するには、**Admin Profiles** ペインで削除するプロファイルを選択し、**Delete** をクリックします。

NetScaler .xva イメージをアップロードする

NetScaler VPX インスタンスを追加するには、**.xva** ファイルが必要です。

VPX インスタンスをプロビジョニングする前に、NetScaler SDX .xva ファイルを SDX アプライアンスにアップロードします。**.xva** イメージファイルをローカルコンピューターにバックアップとしてダウンロードすることもできます。**.xva** イメージファイルの形式は **NSVPX-XEN-ReleaseNumber-BuildNumber_nc** .xva です。

NetScaler XVA Files ペインで、次の詳細を表示できます。

- **名前:** .xva イメージファイルの名前。ファイル名には、リリースとビルド番号が含まれます。たとえば、ファイル名 **NSVPX-XEN-13.1-49.13_nc_64.xva.gz** はリリース 13.1 ビルド 49.13 を指します。
- **最終変更日:** .xva イメージファイルが最後に変更された日付。
- **サイズ:** .xva イメージファイルのサイズ (MB)。

NetScaler .xva ファイルをアップロードするには

1. **Configuration** タブのナビゲーションペインで、**NetScaler Configuration** を展開し、**XVA Files** をクリックします。
2. **NetScaler XVA Files** ペインで、**Upload** をクリックします。
3. **Upload NetScaler instance XVA** ダイアログボックスで、**Browse** をクリックし、アップロードする XVA イメージファイルを選択します。
4. **Upload** をクリックします。アップロード後、XVA イメージファイルが **NetScaler XVA Files** ペインに表示されます。

NetScaler .xva ファイルをダウンロードしてバックアップを作成するには

1. **NetScaler Build Files** ペインで、ダウンロードするファイルを選択し、**Download** をクリックします。
2. **File Download** メッセージボックスで、**Save** をクリックします。

3. **Save As** メッセージボックスで、ファイルを保存する場所を参照し、**Save** をクリックします。

NetScaler インスタンスを追加する

Management Service から NetScaler インスタンスを追加する場合、いくつかのパラメータの値を指定する必要があります。Management Service は、これらの設定を NetScaler インスタンスに自動的に構成します。

SDX インスタンスの詳細(/en-us/sdx/media/sdx-instance-details.png)

- **名前:** NetScaler インスタンスに名前を割り当てます。
- SDX Management Service と VPX インスタンス間の独立した内部常時接続を有効にするには、**Manage through internal network** を選択します。この機能は、SDX アプライアンスで実行されている VPX インスタンスの 13.0-36.27 以降のバージョンでサポートされています。
- 管理目的で NetScaler VPX インスタンスにアクセスするために、IPv4 アドレス、IPv6 アドレス、または IPv4 と IPv6 の両方のアドレスを選択します。NetScaler インスタンスは、管理 IP (NSIP) を 1 つしか持つことができません。NSIP アドレスを削除することはできません。
- IPアドレスにネットマスク、デフォルトゲートウェイ、および管理サービスへのネクストホップを割り当てます。
- VPXがバージョン13.0–88.9または13.1–37.8以降でプロビジョニングされている場合、**ゲートウェイ**および**管理サービスへのネクストホップ**フィールドは、以下のいずれかの条件でオプションになります。
 - **内部ネットワーク経由で管理**が有効になっている場合。
 - 構成されたIPv4アドレスが、管理サービスのIPアドレスと同じサブネットにある場合。



次に、XVAファイル、管理者プロファイル、およびインスタンスの説明を追加します。

注： 高可用性セットアップ（アクティブ-アクティブまたはアクティブ-スタンバイ）の場合、Citrixは2つのNetScaler VPXインスタンスを異なるSDXアプライアンスに構成することを推奨します。セットアップ内のインスタンスが、CPU、メモリ、インターフェイス、1秒あたりのパケット数（PPS）、スループットなどの同一のリソースを持っていることを確認してください。

ライセンス割り当て

このセクションでは、NetScaler用に取得したライセンスを指定します。ライセンスは、Standard、Enterprise、Platinumのいずれかです。

注：アスタリスクは必須フィールドを示します。



帯域幅バースト機能が必要な場合は、**割り当てモード**で**バースト可能**を選択します。詳細については、「[SDXでの帯域幅メータリング](#)」を参照してください。

暗号割り当て

リリース12.1 48.13以降、暗号容量を管理するインターフェイスが変更されました。詳細については、「[暗号容量の管理](#)」を参照してください。

リソース割り当て

SDXで実行されているVPXインスタンスの場合、デフォルトでは管理CPUは1つだけです。リリース14.1ビルド21.x以降、専用コアが2つ以上ある場合、VPXインスタンスをプロビジョニングまたは編集する際に、管理CPUをもう1つ追加できます。この機能には、SDXとVPXの両方がソフトウェアバージョン14.1-21.x以降である必要があります。

リソース割り当てで、合計メモリ、1秒あたりのパケット数、およびCPUを割り当てます。

追加の管理CPUを追加するには：

1. **CPU**リストから****専用 (2コア)****以上を選択します。
2. **追加の管理CPU**を追加オプションを選択します。



CPU: インスタンスに専用コアを割り当てるか、インスタンスが他のインスタンスとコアを共有するようにします。共有を選択した場合、1つのコアがインスタンスに割り当てられますが、リソースが不足している場合は、そのコアが他のインスタンスと共有される可能性があります。CPUコアが再割り当てされた場合は、影響を受けるインスタンスを再起動してください。パフォーマンスの低下を避けるため、CPUコアが再割り当てされたインスタンスを再起動してください。

注:

- インスタンスの場合、設定できる最大スループットは180 Gbpsです。
- 最適なパフォーマンスを得るには、ライセンスに関係なく、パケットエンジン (PE) ごとに4 GBのメモリを割り当てることをお勧めします。例えば、6つのPEを持つVPXには24 GBのメモリが割り当てられている必要があります。

次の表に、サポートされているVPX、シングルバンドルイメージバージョン、およびインスタンスに割り当て可能なコアの数を示します。

プラットフォーム名	合計コア数	VPXプロビジョニング で利用可能な合計コア 数	単一インスタンスに割 り当て可能な最大コア 数
SDX 8015、SDX 8400、および SDX 8600	4	3	3
SDX 8900	8	7	7
SDX 11500、SDX 13500、SDX 14500、SDX 16500、SDX 18500、および SDX 20500	12	10	5
SDX 11515、SDX 11520、SDX 11530、SDX 11540、および SDX 11542	12	10	5
SDX 17500、SDX 19500、および SDX 21500	12	10	5
SDX 17550、SDX 19550、SDX 20550、および SDX 21550	12	10	5
SDX 14020、SDX 14030、SDX 14040、SDX 14060、SDX 14080、および SDX 14100	12	10	5

プラットフォーム名	合計コア数	VPXプロビジョニング で利用可能な合計コア 数	単一インスタンスに割 り当て可能な最大コア 数
SDX 22040、SDX 22060、SDX 22080、SDX 22100、および SDX 22120	16	14	7
SDX 24100 および SDX 24150	16	14	7
SDX 14020 40G、SDX 14030 40G、SDX 14040 40G、SDX 14060 40G、SDX 14080 40G、および SDX 14100 40G	12	10	10
SDX 14020 FIPS、SDX 14030 FIPS、SDX 14040 FIPS、SDX 14060 FIPS、SDX 14080 FIPS、および SDX 14100 FIPS	12	10	5
SDX 14040 40S、SDX 14060 40S、SDX 14080 40S、および SDX 14100 40S	12	10	10
SDX 25100A、25160A、25200A	20	18	9
SDX 25100-40G、25160-40G、25200-40G	20	18	16
SDX 26100、26160、26200、26250	28	26	16

プラットフォーム名	合計コア数	VPXプロビジョニング で利用可能な合計コア 数	単一インスタンスに割 り当て可能な最大コア 数
SDX アプライアンス 26100-50S、 26160-50S、 26200-50S、 26250-50S	28	26	16
SDX アプライアンス 26100-100G、 26160-100G、 26200-100G、 26250-100G	28	26	25
SDX 15000	16	14	14
SDX 15000-50G	16	14	14
SDX 9100	10	9	9
SDX 9200	24	23	23
SDX 16000	32	30	16
SDX 17000	48	46	24

注:

専用コアは、インスタンスで実行されているパケットエンジンの数に対応します。専用コアで作成されたVPXインスタンスの場合、管理用にCPUが追加で割り当てられます。

SDX上のNetScaler VPXで追加の管理CPUを有効にするための推奨事項

NetScaler SDX展開では、各VPXインスタンスは、データプレーン（パケット処理）と管理プレーン（制御および管理操作）の両方のワークロードを処理します。管理アクティビティが高い環境では、管理プレーンでCPU競合が発生し、構成変更、監視、API操作などのタスクの応答性に影響を与える可能性があります。

システムパフォーマンスと安定性を向上させるため、CitrixはSDXプラットフォームで実行されているNetScaler VPXインスタンス向けに、追加の管理CPU（追加の管理スレッドとも呼ばれます）を有効にすることを推奨します。

概要

デフォルトでは、管理プレーンの処理は、利用可能なハイパースレッド全体に分散され、パケットエンジン間でタイムシェアされます。NetScaler 14.1ビルド以降、SDXは、管理プレーンタスク専用の追加の管理ハイパースレッドを有効にすることをサポートしています。

注:

NetScalerバージョン14.1ビルド66.59以降、VPXインスタンスに2つ以上の専用コアを選択すると、追加の管理CPUがデフォルトで割り当てられます。

主な特徴は次のとおりです。

- 追加の管理CPUは、物理コアではなく、ハイパースレッドを使用して実装されます。
- 管理プレーン操作向けに専用の処理能力を提供します。
- 他のプラットフォームで使用されている従来の追加管理CPUの実装とは異なります。

利点:

- 管理プレーンの応答性の向上
 - CLIおよびAPIコマンドの実行の高速化。
 - 構成変更に対する遅延の削減。
 - GUIおよび自動化ワークフローの応答性の向上。
- 安定性の強化
 - 負荷がかかった状態での管理プレーンの競合の可能性を低減します。
 - 高度な監視、ログ記録、または自動化アクティビティによる影響を最小限に抑えます。
- データプレーンのパフォーマンスへの影響なし
 - パケット処理コア（パケットエンジン）は削減または影響を受けません。
 - データプレーンのスループットは変更されません。

前提条件:

追加の管理CPUを有効にする前に、次の前提条件が満たされていることを確認してください。

- **NetScalerバージョン:** SDXおよびVPXインスタンスの両方でNetScaler 14.1-21.x以降。
- **VPXプロビジョニング:** 各VPXインスタンスに少なくとも2つのCPUコアを割り当てる必要があります。
- **プラットフォーム要件:** SDXプラットフォームでハイパースレッディングを有効にする必要があります。

追加の管理CPUを有効にするタイミング

Citrixは、お使いの環境で以下のいずれかの状況が見られる場合に、追加の管理CPUを有効にすることをお勧めします。

高い管理アクティビティ	パフォーマンスに関する懸念
継続的な監視とテレメトリ収集	CLIまたはGUIの応答時間の遅延
頻繁な構成変更または自動化	構成適用時の遅延
高いAPIまたはオーケストレーションアクティビティ	高い管理CPU使用率

注:

管理CPUに負荷がかかっている場合は、この機能を有効にしてください。

運用上の考慮事項:

- 追加の管理CPUを有効または無効にした後、VPXの再起動が必要です。
- 追加の管理CPUの動作は、ハイパーバイザー上のNetScaler MPXおよびNetScaler VPXとは異なります。
- この機能は、SDXで実行されているVPXインスタンスに特に適用されます。

推奨事項の概要:

- 追加の管理CPUを有効にすることは、推奨される低リスクの構成です。
- これにより、管理プレーンのパフォーマンスと信頼性が向上します。
- データプレーンのスループットやパケットエンジンの割り当てには影響しません。
- ほとんどのSDX展開において、ベストプラクティスと見なされています。

インスタンス管理

Instance Administrationの下にある**Add Instance Administration**を選択して、VPXインスタンスの管理者ユーザーを作成できます。



次の詳細を追加します。

ユーザー名: NetScalerインスタンス管理者のユーザー名。このユーザーはスーパーユーザーアクセス権を持っていますが、VLANやインターフェイスを構成するためのネットワークコマンドへのアクセス権はありません。

パスワード: ユーザー名のパスワード。

Shell/Sftp/Scpアクセス: NetScalerインスタンス管理者に許可されるアクセス。このオプションはデフォルトで選択されています。

ネットワーク設定

- **L2モードを許可:** NetScalerインスタンスでL2モードを許可できます。**Networking Settings**の下にある**Allow L2 Mode**を選択します。インスタンスにログオンしてL2モードを有効にする前に。詳細については、「[NetScalerインスタンスでのL2モードの許可](#)」を参照してください。



注:

- Management ServiceからインスタンスのL2モードを無効にする場合は、そのインスタンスにログオンしてL2モードを無効にする必要があります。そうしないと、インスタンスを再起動した後に他のすべてのNetScalerモードが無効になる可能性があります。
- ADCインスタンスがSDXにプロビジョニングされた後、ADCインスタンスからインターフェイスまたはチャンネルを削除することはできません。ただし、ADCインスタンスにインターフェイスまたはチャンネルを追加することはできます。

- **インターフェイス0/1および0/2:** デフォルトでは、インターフェイス0/1と0/2が管理LAに選択されています。
- **VLANタグ:** 管理インターフェイスのVLAN IDを指定します。次に、データインターフェイスを追加します。

注

インスタンスに追加するインターフェイスのインターフェイスIDは、SDXアプライアンスの物理インターフェイス番号と必ずしも一致しません。インスタンス1に関連付ける最初のインターフェイスがインターフェイス1/4である場合、インスタンスのインターフェイス設定を表示すると、インターフェイス1/1として表示されます。これは、インスタンス1に関連付けた最初のインターフェイスであるため、番号付けが変わります。



- **タグなしトラフィックを許可:** **Allow untagged traffic**チェックボックスをオンにして、NetScalerインスタンスがタグなしトラフィックを処理できるようにします。

注:

SDXアプライアンスのバージョンが13.1-24.x以降で、NetScalerインスタンスのバージョンが13.1-24.xより前の場合、**Allow untagged traffic**チェックボックスがオフになっていても、ADCインスタンスはMellanoxインターフェイスでタグなしトラフィックを処理します。

- **許可されたVLAN:** NetScalerインスタンスに関連付けることができるVLAN IDのリストを指定します。
- **MACアドレスモード:** MACアドレスを割り当てます。次のいずれかのオプションを選択します。
 - **デフォルト:** Citrix Hypervisor™ が MAC アドレスを割り当てます。
 - **カスタム:** 生成された MAC アドレスを上書きする MAC アドレスを指定するには、このモードを選択します。
 - **生成済み:** 以前に設定したベース MAC アドレスを使用して MAC アドレスを生成します。ベース MAC アドレスの設定については、「インターフェイスへの MAC アドレスの割り当て」を参照してください。
- **VMAC 設定 (仮想 MAC を構成するための IPv4 および IPv6 VRID)**
 - **VRID IPv4:** VMAC を識別する IPv4 VRID。指定可能な値: 1~255。詳細については、「インターフェイスでの VMAC の構成」を参照してください。

- **VRID IPv6:** VMAC を識別する IPv6 VRID。指定可能な値: 1～255。詳細については、「インターフェイスでの VMAC の構成」を参照してください。

管理 VLAN 設定

通常、管理サービスと VPX インスタンスの管理アドレス (NSIP) は同じサブネットワーク内にあり、通信は管理インターフェイスを介して行われます。ただし、管理サービスとインスタンスが異なるサブネットワークにある場合は、VPX インスタンスのプロビジョニング時に VLAN ID を指定する必要があります。この ID は、インスタンスが起動時にネットワーク経由で到達可能であるために必要です。デプロイで、NSIP が VPX インスタンスのプロビジョニング時に選択されたインターフェイスによってのみアクセス可能である必要がある場合は、NSVLAN オプションを選択します。

NSVLAN オプションが選択されている場合、NetScaler インスタンスをプロビジョニングした後はこの設定を変更できません。

VPX 管理 VLAN 設定(/en-us/sdx/media/vpx-mgmt-vlan-setting.png)

注:

- HA ハートビートは、NSVLAN の一部であるインターフェイスでのみ送信されます。

重要: NSVLAN が選択されていない場合、VPX インスタンスで「clear config full」コマンドを実行すると、VLAN 設定が削除されます。

完了 をクリックして、NetScaler VPX アプライアンスをプロビジョニングします。

NetScaler インスタンスの編集

プロビジョニングされた NetScaler インスタンスのパラメータ値を編集するには:

1. **NetScaler > インスタンス**に移動します。
2. 編集するインスタンスを選択し、**編集**をクリックします。
3. **NetScalerの構成**ページで、値を編集します。

NetScaler インスタンスのゲートウェイフィールドが空白の場合、以下のいずれかの条件でのみインスタンスを編集できます。

- NetScaler インスタンスが管理サービスから到達可能な場合。
- 内部ネットワーク経由で管理が有効になっている場合。

これらの条件は、編集操作中にNetScalerインスタンスが到達可能であることを保証するために課されます。

注:

- VPXインスタンスを編集して管理CPUを1つ追加できるのは、専用コアが2つ以上あり、VPXとSDXの両方がリリース14.1およびビルド21.x以降である場合のみです。
 - リリース14.1-21.xより前のVPXで**追加の管理CPUを追加オプション**を選択すると、エラーが発生します。この機能を使用するには、VPXインスタンスをリリース14.1-21.x以降にアップグレードしてください。
- 
- VPXインスタンスを14.1-21.xより前のビルドにダウングレードする前に、**追加の管理CPUを追加オプション**を無効にする必要があります。そうしないと、VPXインスタンスのパフォーマンスに影響が出ます。
 - **追加の管理CPUを追加オプション**が無効になっておらず、VPXインスタンスが14.1-21.xより前のバージョンにダウングレードされた場合、アラームが生成されます。

注意点:

- SSLチップ数、インターフェース、メモリ、機能ライセンスなどのパラメータを変更すると、NetScalerインスタンスはこれらのパラメータを有効にするために暗黙的に停止し、再起動します。
- イメージとユーザー名のパラメータは変更できません。
- インターフェースまたはチャンネルはADCインスタンスから削除できません。ただし、新しいインターフェースまたはチャンネルをADCインスタンスに追加することはできます。
- SDXアプライアンスにプロビジョニングされたADCインスタンスを削除するには、**NetScaler インスタンスペイン**で、削除するインスタンスを選択し、**削除**をクリックします。**確認メッセージ**ボックスで、**はい**をクリックしてNetScalerインスタンスを削除します。

VLANを特定の仮想インターフェースに制限する

SDXアプライアンスの管理者は、NetScalerインスタンスに関連付けられた仮想インターフェースに特定の802.1Q VLANを適用できます。この機能は、インスタンス管理者による802.1Q VLANの使用を制限するのに特に役立ちます。2つの異なる企業に属する2つのインスタンスがSDXアプライアンスでホストされている場合、両社が同じVLAN IDを使用することを制限できます。これによ

り、一方の企業が他方の企業のトラフィックを見ることはありません。インスタンス管理者がインターフェースを802.1Q VLANに割り当てようとする、指定されたVLAN IDが許可リストの一部であることを確認するための検証が実行されます。

デフォルトでは、任意のVLAN IDをインターフェースで使用できます。インターフェース上のタグ付きVLANを制限するには、NetScalerインスタンスのプロビジョニング時にネットワーク設定でVLAN IDを指定します。後でインスタンスを変更して指定することもできます。範囲を指定するには、ハイフンでIDを区切ります（例：10–12）。最初にいくつかのVLAN IDを指定したが、後で許可リストからすべて削除した場合、そのインターフェースで任意のVLAN IDを使用できます。これは実質的に、デフォルト設定に戻したことになります。

許可されたVLANのリストを作成した後、SDX管理者はVLANを作成するためにインスタンスにログオンする必要はありません。管理者は、Management Serviceから特定のインスタンスのVLANを追加および削除できます。

重要：L2モードが有効になっている場合、管理者は異なるNetScalerインスタンス上のVLAN IDが重複しないように注意する必要があります。

許可されたVLAN IDを指定するには

1. ADCプロビジョニングウィザードまたはADC変更ウィザードのネットワーク設定ページで、**許可されたVLAN**に、このインターフェースで許可される1つ以上のVLAN IDを指定します。範囲を指定するにはハイフンを使用します。例：2–4094。
2. ウィザードの指示に従います。
3. **完了**をクリックし、次に**閉じる**をクリックします。

Management ServiceからインスタンスのVLANを構成するには

1. **構成**タブで、NetScaler > インスタンスに移動します。
2. インスタンスを選択し、次に**VLAN**をクリックします。
3. 詳細ペインで、**追加**をクリックします。
4. **NetScaler VLANの作成**ダイアログボックスで、次のパラメータを指定します。
 - **VLAN ID** — 特定のフレームが属するVLANを一意に識別する整数。NetScalerは最大4094のVLANをサポートします。ID 1はデフォルトVLAN用に予約されています。
 - **IPv6動的ルーティング** — このVLANで、すべてのIPv6動的ルーティングプロトコルを有効にします。注: **ENABLED**設定を機能させるには、インスタンスにログオンし、VTYSHコマンドラインからIPv6動的ルーティングプロトコルを設定する必要があります。

5. VLANの一部である必要があるインターフェイスを選択します。
6. **作成**をクリックし、次に**閉じる**をクリックします。

暗号容量の管理

Management Service は、NetScaler SDX アプライアンス上の SSL 容量を示すために、非対称暗号ユニット (ACU)、対称暗号ユニット (SCU)、および暗号仮想インターフェイスを提供します。以前は、暗号容量は SSL チップ、SSL コア、および SSL 仮想機能の単位で割り当てられていました。レガシー SSL チップが ACU および SCU ユニットのどのように変換されるかの詳細については、[レガシー SSL チップから ACU および SCU への変換表](#) を参照してください。

Management Service GUI を使用して、ACU および SCU 単位で NetScaler VPX インスタンスに暗号容量を割り当てることができます。

次の表は、ACU、SCU、および暗号仮想インスタンスに関する簡単な説明を示しています。

表。単位暗号ユニット

新しい暗号ユニット	説明
非対称暗号ユニット (ACU)	1 ACU = (RSA) 2 K (2048 ビット鍵サイズ) 復号化の 1 秒あたり 1 オペレーション (ops)。詳細については、 ACU から PKE リソースへの変換表 を参照してください。
対称暗号ユニット (SCU)	1 SCU = AES-128-CBC + SHA256-HMAC @ 1024B の 1 Mbps。この定義は、すべての SDX プラットフォームに適用されます。
暗号仮想インターフェイス	仮想機能とも呼ばれる暗号仮想インターフェイスは、SSL ハードウェアの基本単位を表します。これらのインターフェイスが使い果たされると、SSL ハードウェアを VPX インスタンスにさらに割り当てることはできません。暗号仮想インターフェイスは読み取り専用エンティティであり、SDX アプライアンスがこれらのエンティティを自動的に割り当てます。

SDX アプライアンスの暗号容量を表示する

SDX GUI のダッシュボードで、SDX アプライアンスの暗号容量を表示できます。ダッシュボードには、SDX アプライアンスで使用済みおよび利用可能な ACU、SCU、および仮想インターフェイスが表示されます。暗号容量を表示するには、**ダッシュボード > 暗号容量** に移動します。

暗号容量を表示(/en-us/sdx/media/view-crypto-capacity.png)

VPXインスタンスのプロビジョニング中に暗号容量を割り当てる

SDXアプライアンスでVPXインスタンスをプロビジョニングする際に、「**Crypto Allocation**」の下で、VPXインスタンスに割り当てるACUとSCUの数を指定できます。VPXインスタンスのプロビジョニング手順については、「[NetScalerインスタンスのプロビジョニング](#)」を参照してください。

VPXインスタンスのプロビジョニング中に暗号容量を割り当てるには、次の手順に従います。

1. Management Serviceにログオンします。
2. **Configuration > NetScaler > Instances**に移動し、**Add**をクリックします。
3. 「**Crypto Allocation**」の下で、利用可能なACU、SCU、および暗号仮想インターフェイスを表示できます。ACUとSCUの割り当て方法は、SDXアプライアンスによって異なります。
 - a. [さまざまなSDXアプライアンスで利用可能なACUカウンターの最小値](#)に記載されているアプライアンスの場合、指定された数の倍数でACUを割り当てることができます。SCUは自動的に割り当てられ、SCU割り当てフィールドは編集できません。そのモデルで利用可能な最小ACUの倍数でACU割り当てを増やすことができます。たとえば、最小ACUが4375の場合、ACUの増分は8750、13125などになります。

例。 SCUが自動的に割り当てられ、ACUが指定された数の倍数で割り当てられる暗号割り当て。

暗号割り当て(/en-us/sdx/media/image003.png)

さまざまなSDXアプライアンスで利用可能なACUカウンターの最小値

SDXプラットフォーム	ACUカウンターの最小値
22040, 22060, 22080, 22100, 22120, 24100, 24150 (36 ポート	2187

SDXプラットフォーム	ACUカウンターの最小値
8400, 8600, 8010, 8015	2812
17500, 19500, 21500	2812
17550, 19550, 20550, 21550	2812
11500, 13500, 14500, 16500, 18500, 20500	2812
11515, 11520, 11530, 11540, 11542	4375
14xxx	4375
14xxx 40エス	4375
14xxx 40ジー	4375
14xxx FIPS	4375
25xxx	4375
25xxx エー	4575

b. 前の表に記載されていないその他のSDXプラットフォームについては、ACUとSCUを自由に割り当てることができます。SDXアプライアンスは、暗号仮想インターフェイスを自動的に割り当てます。

例。 ACUとSCUの両方が自由に割り当てられる暗号割り当て



4./ VPXインスタンスをプロビジョニングするためのすべての手順を完了し、完了をクリックします。詳細については、「[NetScalerインスタンスのプロビジョニング](#)」を参照してください。

暗号ハードウェアの健全性を表示

Management Serviceでは、SDXアプライアンスに付属の暗号ハードウェアの健全性を表示できます。暗号ハードウェアの健全性は、暗号デバイスと暗号仮想機能として表されます。暗号ハードウェアの健全性を表示するには、**ダッシュボード > リソース**に移動します。



注意事項

SDXアプライアンスを最新バージョンにアップグレードする際は、以下の点に注意してください。

- SDXユーザーインターフェイスのみがアップグレードされ、アプライアンスのハードウェア容量は同じままです。
- 暗号割り当てメカニズムは同じままであり、SDX GUIでの表示のみが変更されます。
- 暗号インターフェイスは下位互換性があり、NITROインターフェイスを使用してSDXアプライアンスを管理する既存の自動化メカニズムには影響しません。
- SDXアプライアンスのアップグレード後も、既存のVPXインスタンスに割り当てられた暗号は変更されず、Management Serviceでの表示のみが変更されます。

ACUからPKEリソースへの変換テーブル

SDXプラットフォーム	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE-ECDSA
22040, 22060, 22080, 22100, 22120, 24100, 24150 (36ポート)	2187	12497	2187	312	256	190
8400, 8600, 8010, 8015	2812	17000	2812	424	330	該当なし
11515, 11520, 11530, 11540, 11542	4375	25000	4375	625	512	381
22040, 22060, 22080,22	4375	25000	4375	625	512	381

SDXプラットフォーム	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE-ECDSA
100, 22120 (24 ポート)						
17500, 19500, 21500	2812	17000	2812	424	330	N/A
17550, 19550, 20550, 21550	2812	17000	2812	424	330	N/A
11500, 13500, 14500, 16500, 18500, 20500	2812	17000	2812	424	330	N/A
14000, 14000-40 G, 25000, 25000A	4375	25000	4375	625	512	381
14000 FIPS	4375	25000	4375	625	512	381
14000-40 S	4375	25000	4375	625	512	381
*8900 (8910, 8920, 8930)	1000	4615	1000	136	397	494
*9100 (9110, 9120, 9130)	1000	4615	1000	136	397	494

SDXプラットフォーム	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE-ECDSA
*26000-100G (26100, 26160, 26200、および26250)	1000	4615	1000	136	397	494
*15000	1000	4615	1000	136	397	494
*15000-50G	1000	4615	1000	136	397	494
*16000	1000	4615	1000	136	397	494
*26000-50S	1000	4615	1000	136	397	494
*17000	1000	3070	1000	99	859	2388
*9200	1000	3070	1000	99	859	2388

*これらのプラットフォームでは、PKEの数値は保証される最小値です。

ACUからPKEへのリソース変換テーブルの読み方

ACUからPKEへのリソース変換テーブルは、以下の点に基づいています。

- Management Serviceは、個々のVPXに暗号リソースを割り当てするのに役立ちます。
Management Serviceは、パフォーマンスを割り当てたり保証したりすることはできません。
- 実際のパフォーマンスは、パケットサイズ、使用される暗号/Keyex/HMAC（またはそのバリエーション）などによって異なります。

以下の例は、ACUからPKEリソースへの変換テーブルの読み方と適用方法を理解するのに役立ちます。

例: SDX 22040プラットフォームにおけるACUからPKEリソースへの変換。

SDX 22040プラットフォーム上のVPXインスタンスに2187 ACUを割り当てると、256のECDHE-RSA操作または2187のRSA-2K操作などに相当する暗号リソースが割り当てられます。

レガシーSSLチップからACUおよびSCUへの変換テーブル

レガシーSSLチップがACUおよびSCUに変換される方法の詳細については、以下の表を参照してください。

[ACUおよびSCU変換テーブル](#)

サードパーティ製仮想マシンのプロビジョニング

注:

バージョン14.1ビルド17.x以降、NetScaler SDXはサードパーティ製仮想マシンのサポートを終了しました。

SDXアプライアンスは、以下のサードパーティ製仮想マシン（インスタンス）のプロビジョニングをサポートしています。

- SECUREMATRIX GSB
- インタースキャン ウェブセキュリティ
- ウェブセンス プロテクター
- ブルーキャット DNS/DHCP サーバー
- CA アクセス ゲートウェイ
- パロアルト VMシリーズ

SECUREMATRIX GSBは、トークンデバイスを持ち運ぶ必要のない、高度に安全なパスワードシステムを提供します。Websense Protectorは、監視およびブロック機能を提供し、データ損失や機密情報の漏洩を防ぎます。BlueCat DNS/DHCP Serverは、ネットワークにDNSとDHCPを提供します。NetScaler SDX上のPaloAlto VM-Seriesは、単一プラットフォームで高度なセキュリティとADC機能を統合し、企業やサービスプロバイダーの顧客によるアプリケーションへの安全で信頼性の高いアクセスを可能にします。NetScaler SDX上のVM-Seriesの組み合わせは、Citrix Virtual Apps and Desktopsの展開向けに、完全で検証済みの安全なADCソリューションも提供します。

Management Serviceからインスタンスをプロビジョニング、監視、管理、トラブルシューティングできます。上記のすべてのサードパーティインスタンスは、Management Serviceと通信するために **SDXTools** デーモンを使用します。デーモンはプロビジョニングされたインスタンスにプリインストールされています。新しいバージョンが利用可能になったときに、デーモンをアップグレードできます。

サードパーティ製仮想マシンを構成する場合、チャンネルの一部であるSR-IOVインターフェイス（1/xおよび10/x）はインターフェイスのリストに表示されません。チャンネルはサードパーティ製仮想マシンでサポートされていないため、インターフェイスがありません。

注:

SDXアプライアンスでプロビジョニングできるインスタンスの総数は、アプライアンスにインストールされているライセンスによって異なります。

重要: サードパーティ製インスタンスをインストールする前に、Citrix Hypervisor のバージョンをバージョン 6.1.0 にアップグレードする必要があります。

SECUREMATRIX GSB

注記:

バージョン14.1ビルド17.x以降、NetScaler SDXはサードパーティ製仮想マシンのサポートを終了しました。

SECUREMATRIX は、使いやすく費用対効果の高い、非常に安全なトークンレスのワンタイムパスワード (OTP) 認証ソリューションです。マトリックス表から位置、シーケンス、および画像パターンを組み合わせて使用し、使い捨てパスワードを生成します。SECUREMATRIX GSB サーバーと SECUREMATRIX Authentication サーバーを組み合わせることで、VPN/SSL-VPN エンドポイント、クラウドベースのアプリケーションとリソース、デスクトップ/仮想デスクトップログイン、および Web アプリケーション (OTP を使用したリバースプロキシ) のセキュリティが大幅に強化されます。PC、仮想デスクトップ、タブレット、スマートフォンと互換性のあるソリューションを提供します。

ソフトウェア定義ネットワークにおける NetScaler SDX のマルチテナントプラットフォームアーキテクチャを使用することで、SECUREMATRIX の強力な認証機能を、Web Interface、Citrix Virtual Apps and Desktops、その他多くの認証を必要とするアプリケーションサービスなど、NetScaler を介して提供される他のテナントやクラウドサービスと統合できます。

SECUREMATRIX GSB インスタンスをプロビジョニングする

SECUREMATRIX GSB には、SDX アプライアンスの外部で構成する必要がある SECUREMATRIX Authentication サーバーが必要です。インターフェイスを正確に1つ選択し、そのインターフェイスのみのネットワーク設定を指定してください。

注記: チャンネルの一部である SR-IOV インターフェイス (1/x および 10/x) は、インターフェイスのリストに表示されません。チャンネルは SECUREMATRIX GSB インスタンスではサポートされていません。

インスタンスのプロビジョニングを開始する前に、SECUREMATRIX の Web サイトから XVA イメージをダウンロードし、SDX アプライアンスにアップロードしてください。XVA イメージのダウンロードの詳細については、SECUREMATRIX の Web サイトを参照してください。SDX アプライアンスで Management Service ビルド 118.7 以降を使用していることを確認してください。

Configuration タブで、**SECUREMATRIX GSB > Software Images** に移動します。

XVA イメージを SDX アプライアンスにアップロードするには:

1. 詳細ペインの **XVA Files > Action** で、**Upload** をクリックします。
2. 表示されるダイアログボックスで、**Browse** をクリックし、アップロードする XVA ファイルを選択します。
3. **Upload** をクリックします。XVA ファイルが XVA Files ペインに表示されます。

SECUREMATRIX インスタンスをプロビジョニングするには

1. 「**Configuration**」タブで、「**SECUREMATRIX GSB > Instances**」に移動します。
2. 詳細ペインで、「**Add**」をクリックします。
3. 「**Provision SECUREMATRIX GSB wizard**」で、画面の指示に従います。
4. 「**Finish**」をクリックし、次に「**Close**」をクリックします。

インスタンスをプロビジョニングした後、インスタンスにログオンし、詳細な構成を実行します。

プロビジョニングされた SECUREMATRIX インスタンスの設定を変更するには、

「**SECUREMATRIX Instances**」ペインで、変更するインスタンスを選択し、「**Modify**」をクリックします。「**Modify SECUREMATRIX GSB wizard**」で、パラメーターを変更します。

注: インターフェイスパラメーターまたはインスタンスの名前を変更すると、変更を有効にするためにインスタンスが停止して再起動します。

テクニカルサポートに提出するための tar アーカイブを生成します。テクニカルサポートファイルの生成については、「[テクニカルサポート用の Tar アーカイブの生成](#)」を参照してください。

SECUREMATRIX GSB インスタンスの構成をバックアップし、後でそのバックアップデータを使用して SDX アプライアンス上のインスタンスの構成を復元します。インスタンスのバックアップと復元については、「[SDX アプライアンスの構成データのバックアップと復元](#)」を参照してください。

SECUREMATRIX GSBインスタンスを監視する

SDXアプライアンスは、SECUREMATRIX GSBインスタンスの **SDXTools** のバージョン、SSHおよびCRONデーモンの状態、Webサーバーの状態などの統計情報を収集します。

SECUREMATRIX GSBインスタンスに関連する統計情報を表示するには：

1. 「**SECUREMATRIX GSB > Instances**」に移動します。
2. 詳細ペインで、インスタンス名の横にある矢印をクリックします。

SECUREMATRIX GSBインスタンスを管理する

管理サービスからSECUREMATRIX GSBインスタンスを起動、停止、再起動、強制停止、または強制再起動できます。

構成タブで、**SECUREMATRIX GSB**を展開します。

インスタンスを起動、停止、再起動、強制停止、または強制再起動するには：

1. インスタンスをクリックします。
2. 詳細ペインで、操作を実行するインスタンスを選択し、次のいずれかのオプションを選択します。
 - 起動
 - シャットダウン
 - 再起動
 - 強制シャットダウン
 - 強制再起動
3. 確認メッセージボックスで、**はい**をクリックします。

SECUREMATRIX GSBインスタンスのSDXツールファイルをアップグレードする

SECUREMATRIX GSBインスタンスで実行されているデーモンである **SDXTools** は、管理サービスとインスタンス間の通信に使用されます。

SDXTools のアップグレードには、ファイルをSDXアプライアンスにアップロードし、インスタンスを選択した後に **SDXTools** をアップグレードすることが含まれます。クライアントコンピュータからSDXアプライアンスに **SDXTools** ファイルをアップロードできます。

SDXToolsファイルをアップロードするには：

1. ナビゲーションペインで、**Management Service**を展開し、**SDXTools Files**をクリックします。
2. 詳細ペインで、**Action**リストから**Upload**を選択します。
3. **Upload SDXTools Files**ダイアログボックスで、**Browse**をクリックし、ファイルが含まれているフォルダーに移動して、ファイルをダブルクリックします。
4. **Upload**をクリックします。

SDXToolsをアップグレードするには：

Configurationタブで、**SECUREMATRIX GSB**を展開します。

1. **Instances**をクリックします。
2. 詳細ペインで、インスタンスを選択します。
3. **Action**リストから、**Upgrade SDXTools**を選択します。
4. **Upgrade SDXTools**ダイアログボックスで、ファイルを選択し、**OK**をクリックして、**Close**をクリックします。

SECUREMATRIX GSBインスタンスのアップグレードとダウングレード

SECUREMATRIX GSBインスタンスをアップグレードするプロセスには、ターゲットビルドのソフトウェアイメージをSDXアプライアンスにアップロードし、その後インスタンスをアップグレードする作業が含まれます。ダウングレードでは、インスタンスの以前のバージョンがロードされます。

Configurationタブで、**SECUREMATRIX GSB**を展開します。

ソフトウェアイメージをアップロードするには：

1. **Software Images**をクリックします。
2. 詳細ペインで、**アクション**リストから**アップロード**を選択します。
3. ダイアログボックスで、**参照**をクリックし、ビルドファイルを含むフォルダーに移動して、ビルドファイルをダブルクリックします。
4. **アップロード**をクリックします。

インスタンスをアップグレードするには：

1. **インスタンス**をクリックします。
2. 詳細ペインで、インスタンスを選択します。

3. **アクション**リストから**アップグレード**を選択します。
4. 表示されるダイアログボックスで、ファイルを選択し、**OK**をクリックしてから、**閉じる**をクリックします。

インスタンスをダウングレードするには:

1. **インスタンス**をクリックします。
2. 詳細ペインで、インスタンスを選択します。
3. **アクション**リストから**ダウングレード**を選択します。
4. 確認メッセージボックスで、**はい**をクリックします。

SECUREMATRIX GSB インスタンスのトラブルシューティング

Management Service から SECUREMATRIX GSB インスタンスに ping を実行して、デバイスに到達可能かどうかを確認します。Management Service からインスタンスへのパケットのルートをトレースして、インスタンスに到達するまでにかかるホップ数を特定できます。

インスタンスを再検出して、インスタンスの最新の状態と構成を表示します。再検出中に、Management ServiceはSDXアプライアンスで実行されているSECUREMATRIX GSBの構成とバージョンを取得します。デフォルトでは、Management Serviceは30分に1回、インスタンスの再検出をスケジュールします。

Configurationタブで、**SECUREMATRIX GSB**を展開します。

インスタンスをpingするには：

1. **Instances**をクリックします。
2. 詳細ペインで、pingするインスタンスを選択し、**Action**リストから**Ping**をクリックします。Pingメッセージボックスに、pingが成功したかが表示されます。

インスタンスのルートをトレースするには：

1. **Instances**をクリックします。
2. 詳細ペインで、ルートをトレースするインスタンスを選択し、**Action**リストから**TraceRoute**をクリックします。Tracerouteメッセージボックスに、インスタンスへのルートが表示されます。

インスタンスを再検出するには：

1. **Instances**をクリックします。

2. 詳細ペインで、再検出するインスタンスを選択し、**Action**リストから**Rediscover**をクリックします。
3. 確認メッセージボックスで、**Yes**をクリックします。

トレンドマイクロ InterScan Web Security

注：

バージョン14.1ビルド17.x以降、NetScaler SDXはサードパーティ製仮想マシンのサポートを終了しました。

Trend Micro InterScan Web Securityは、インターネットゲートウェイで従来のWeb脅威と新たなWeb脅威から動的に保護するソフトウェア仮想アプライアンスです。アプリケーション制御、アンチマルウェアスキャン、リアルタイムWebレピュテーション、柔軟なURLフィルタリング、および高度な脅威保護を統合しています。その結果、優れた保護機能と、ネットワーク上でのクラウドベースアプリケーションの使用増加に対する高い可視性と制御を提供します。リアルタイムレポートと集中管理により、管理者はプロアクティブな意思決定ツールを手に入れ、その場でのリスク管理を可能にします。

インタースキャン ウェブセキュリティ：

- エンドユーザーのインターネットアクティビティに対するより深い可視性を可能にします
- 最大限の制御のために管理を集中化します
- Webの使用状況をリアルタイムで監視します
- その場での修復を可能にします
- アプライアンスの乱立とエネルギーコストを削減します
- オプションのデータ損失防止とサンドボックス実行分析を提供します

InterScan Web Securityインスタンスをプロビジョニングする前に、トレンドマイクロのWebサイトからXVAイメージをダウンロードする必要があります。XVAイメージをダウンロードしたら、NetScaler SDXアプライアンスにアップロードします。

****注：****チャネルの一部であるSR-IOVインターフェース（1/xおよび10/x）は、インターフェースのリストには表示されません。チャネルはInterScan Web Securityインスタンスではサポートされていません。

XVAイメージをSDXアプライアンスにアップロードするには：

1. **Configuration**タブから、**TrendMicro IWSVA > Software Images**に移動します。
2. 詳細ペインの「**XVAファイル**」タブで、「**アップロード**」をクリックします。
3. 表示されるダイアログボックスで、「**参照**」をクリックし、アップロードするXVAファイルを選択します。
4. 「**アップロード**」をクリックします。XVAファイルがXVAファイルペインに表示されます。

TrendMicro IWSVAインスタンスをプロビジョニングするには：

1. 「**構成**」タブで、「**TrendMicro IWSVA > インスタンス**」に移動します。
2. 詳細ペインで、「**追加**」をクリックします。
3. 「**TrendMicro IWSVAのプロビジョニング**」ウィザードで、画面の指示に従います。
4. 「**OK**」をクリックし、その後「**閉じる**」をクリックします。

インスタンスをプロビジョニングした後、インスタンスにログオンし、詳細な構成を実行します。

プロビジョニングされたインスタンスのパラメーターの値を変更するには、詳細ペインで変更するインスタンスを選択し、その後「**編集**」をクリックします。「**TrendMicro IWSVAの変更**」ウィザードで、環境に適した値にパラメーターを設定します。

ウェブセンス プロテクター

注：

バージョン14.1ビルド17.x以降、NetScaler SDXはサードパーティ製仮想マシンのサポートを終了しました。

Websense（現在はForcepointとして知られています）のData Securityプロテクターは、送信HTTPトラフィック（投稿）を傍受する仮想マシンです。その後、トラフィックを分析して、Web経由でのデータ損失や機密データの漏洩を防ぎます。プロテクターは、DLPポリシー情報のために専用のWindowsサーバーと通信し、一致が検出された場合にデータの投稿を監視またはブロックできます。コンテンツ分析はボックス内で実行されるため、このプロセス中に機密データがプロテクターから離れることはありません。

プロテクターのデータ損失防止（DLP）機能を使用するには、次の手順を実行します。

- Websense Data Securityを購入してインストールする
- Data SecurityマネージャーでWeb DLPポリシーを設定する
- 管理サービスを通じて初期設定を実行する。

WebSense Protectorインスタンスをプロビジョニングする

WebSense Protectorには、SDXアプライアンスの外部で構成する必要があるData Security Management Serverが必要です。管理インターフェイスを1つ、データインターフェイスを2つ正確に選択します。データインターフェイスには、を選択する必要があります。Data Security Management ServerがWebSense Protectorの管理ネットワーク経由でアクセスできることを確認してください。ネームサーバーには、このプロテクターにサービスを提供するドメインネームサーバー（DNS）のIPアドレスを入力します。

****注：****チャンネルの一部であるSR-IOVインターフェイス（1/xおよび10/x）は、インターフェイスのリストには表示されません。チャンネルはWebSense Protectorインスタンスではサポートされていません。

インスタンスのプロビジョニングを開始する前に、WebSenseのWebサイトからプロテクターイメージをダウンロードし、SDXアプライアンスにアップロードしてください。プロテクターイメージのダウンロードの詳細については、WebSenseのWebサイトを参照してください。SDXアプライアンスでManagement Serviceビルド118.7以降を使用していることを確認してください。

Configurationタブで、**WebSense Protector > Software Images**に移動します。

XVAイメージをSDXアプライアンスにアップロードするには

1. 詳細ペインの**XVA Files > Action**で、**Upload**をクリックします。
2. 表示されるダイアログボックスで、をクリックし、アップロードするXVAファイルを選択します。
3. **アップロード**をクリックします。XVAファイルがXVAファイルペインに表示されます。

WebSense Protectorインスタンスをプロビジョニングするには

1. **構成**タブで、**WebSense Protector > インスタンス**に移動します。
2. 詳細ペインで、**追加**をクリックします。
3. **WebSense Protectorのプロビジョニングウィザード**で、画面の指示に従います。
4. **完了**をクリックし、次に**閉じる**をクリックします。

インスタンスをプロビジョニングした後、インスタンスにログオンし、詳細な構成を実行します。

プロビジョニングされたWebSense Protectorインスタンスの設定を変更するには、WebSense Protectorインスタンスペインで、変更するインスタンスを選択し、**変更**をクリックします。

WebSense Protectorの変更ウィザードで、パラメーターを設定します。WebSenseインスタンスの

プロビジョニング時に選択されたインターフェースは変更しないでください。XVAファイルは、インスタンスを削除して新しいインスタンスをプロビジョニングした後にのみ変更できます。

テクニカルサポートに提出するためのtarアーカイブを生成できます。テクニカルサポートファイルの生成については、[テクニカルサポート用のTarアーカイブの生成](#)を参照してください。

Websense Protectorインスタンスを監視する

SDXアプライアンスは、`SDXTools` のバージョン、Websense Data Securityポリシーエンジンのステータス、Data Securityプロキシのステータスなどの統計情報を収集します。

Websense Protectorインスタンスに関連する統計情報を表示するには：

1. **Websense Protector > インスタンス**に移動します。
2. 詳細ペインで、インスタンス名の横にある矢印をクリックします。

Websense Protectorインスタンスを管理する

Management ServiceからWebsense Protectorインスタンスを開始、停止、再起動、強制停止、または強制再起動できます。

Configurationタブで、**Websense Protector**を展開します。

Websense Protectorインスタンスを開始、停止、再起動、強制停止、または強制再起動するには

1. **Instances**をクリックします。
2. 詳細ペインで、操作を実行するインスタンスを選択し、次のいずれかのオプションを選択します。
 - 開始
 - シャットダウン
 - 再起動
 - 強制シャットダウン
 - 強制再起動
3. 確認メッセージボックスで、**Yes**をクリックします。

Websense ProtectorインスタンスのSDXツールファイルをアップグレードする

サードパーティインスタンスで実行されているデーモンである **SDXTools** は、Management Serviceとサードパーティインスタンス間の通信に使用されます。

SDXTools のアップグレードには、ファイルをSDXアプライアンスにアップロードし、インスタンスを選択した後に **SDXTools** をアップグレードする作業が含まれます。クライアントコンピュータからSDXアプライアンスに **SDXTools** ファイルをアップロードできます。

SDXツールファイルをアップロードするには

1. ナビゲーションペインで、**Management Service** を展開し、**SDXTools Files** をクリックします。
2. 詳細ペインで、**Action** リストから **Upload** を選択します。
3. **Upload SDXTools Files** ダイアログボックスで、**Browse** をクリックし、ファイルが含まれているフォルダに移動して、ファイルをダブルクリックします。
4. **Upload** をクリックします。

SDXツールをアップグレードするには

Configuration タブで、**Websense Protector** を展開します。

1. **Instances** をクリックします。
2. 詳細ペインで、インスタンスを選択します。
3. **Action** リストから **Upgrade SDXTools** を選択します。
4. **Upgrade SDXTools** ダイアログボックスで、ファイルを選択し、**OK** をクリックしてから、**Close** をクリックします。

Websense Protectorインスタンスを新しいバージョンにアップグレードする

Websense Protectorインスタンスをアップグレードするプロセスには、ターゲットビルドのソフトウェアイメージをSDXアプライアンスにアップロードし、その後インスタンスをアップグレードする作業が含まれます。

Configuration タブで、**Websense Protector** を展開します。

ソフトウェアイメージをアップロードするには

1. 「ソフトウェアイメージ」をクリックします。

2. 詳細ペインで、「アクション」リストから「アップロード」を選択します。
3. ダイアログボックスで「参照」をクリックし、ビルドファイルを含むフォルダーに移動して、ビルドファイルをダブルクリックします。
4. 「アップロード」をクリックします。

インスタンスをアップグレードするには

1. 「インスタンス」をクリックします。
2. 詳細ペインでインスタンスを選択します。
3. 「アクション」リストから「アップグレード」を選択します。
4. 表示されるダイアログボックスでファイルを選択し、「OK」をクリックしてから「閉じる」をクリックします。

Websense Protectorインスタンスのトラブルシューティング

Management ServiceからWebsense Protectorインスタンスにpingを実行して、デバイスに到達可能かどうかを確認します。Management Serviceからインスタンスへのパケットのルートをトレースして、インスタンスに到達するまでにかかるホップ数を特定できます。

インスタンスを再検出して、インスタンスの最新の状態と構成を表示します。再検出中に、Management ServiceはSDXアプライアンスで実行されているWebsense Protectorの構成とバージョンを取得します。デフォルトでは、Management Serviceは30分ごとにインスタンスの再検出をスケジュールします。

「構成」タブで、「Websense Protector」を展開します。

インスタンスにpingを実行するには

1. 「インスタンス」をクリックします。
2. 詳細ペインで、pingするインスタンスを選択し、アクションリストから**Ping**をクリックします。Pingメッセージボックスに、pingが成功したかどうかが表示されます。

インスタンスのルートをトレースするには

1. インスタンスをクリックします。
2. 詳細ペインで、ルートをトレースするインスタンスを選択し、アクションリストから**TraceRoute**をクリックします。Tracerouteメッセージボックスに、インスタンスへのルートが表示されます。

インスタンスを再検出するには

1. インスタンスをクリックします。
2. 詳細ペインで、再検出するインスタンスを選択し、アクションリストから**Rediscover**をクリックします。
3. 確認メッセージボックスで、**はい**をクリックします。

BlueCat DNS/DHCP

注：

バージョン14.1ビルド17.x以降、NetScaler SDXはサードパーティ製仮想マシンのサポートを終了しました。

BlueCat DNS/DHCP Serverは、NetScaler SDXアプライアンスによってサポートされるソフトウェアソリューションです。NetScaler SDXプラットフォームでホストされ、追加の管理コストやデータセンターのスペースを発生させることなく、信頼性が高く、スケーラブルで、安全なDNSおよびDHCPコアネットワークサービスを提供します。重要なDNSサービスは、追加のハードウェアを必要とせずに、単一システム内の複数のDNSノード間、または複数のSDXアプライアンス間でロードバランスできます。

BlueCat DNS/DHCP Serverの仮想インスタンスはSDX上でホストでき、モバイルデバイス、アプリケーション、仮想環境、クラウドを接続するためのよりスマートな方法を提供します。

BlueCatとCitrixについて詳しく知るには、BlueCatのウェブサイト [<https://citrixready.citrix.com/bluecat-networks.html>](https://citrixready.citrix.com/bluecat-networks.html) をご覧ください。

既存のBlueCatのお客様は、BlueCatサポートポータル [<https://care.bluecatnetworks.com/>](https://care.bluecatnetworks.com/) からソフトウェアとドキュメントをダウンロードできます。

BlueCat DNS/DHCPインスタンスのプロビジョニング

BlueCatカスタマーケアの [<https://care.bluecatnetworks.com>](https://care.bluecatnetworks.com) からXVAイメージをダウンロードします。XVAイメージをダウンロードしたら、インスタンスのプロビジョニングを開始する前にSDXアプライアンスにアップロードします。SDXアプライアンスでManagement Serviceビルド118.7以降を使用していることを確認してください。

0/1および0/2インターフェイスを介した管理チャネルは、BlueCat DNS/DHCP VMでサポートされています。詳細については、「[Management Serviceからのチャネルの構成](#)」を参照してください。

注：チャンネルの一部であるSR-IOVインターフェイス（1/xおよび10/x）は、BlueCat DNS/DHCPインスタンスではチャンネルがサポートされていないため、インターフェイスのリストに表示されません。

Configurationタブで、**BlueCat DNS/DHCP > Software Images**に移動します。

XVAイメージをSDXアプライアンスにアップロードするには：

1. 詳細ペインの**XVA Files > Action**で、**Upload**をクリックします。
2. 表示されるダイアログボックスで、**参照**をクリックし、アップロードするXVAファイルを選択します。
3. 「**アップロード**」をクリックします。XVAファイルがXVAファイルペインに表示されます。

BlueCat DNS/DHCPインスタンスをプロビジョニングするには：

1. 構成タブで、BlueCat DNS/DHCP > インスタンスに移動します。
2. 詳細ペインで、「**追加**」をクリックします。BlueCat DNS/DHCPサーバーのプロビジョニングページが開きます。
3. BlueCat DNS/DHCPプロビジョニングウィザードで、画面の指示に従います。
 - インスタンス作成で、名前フィールドにインスタンスの名前を入力し、XVAファイルドロップダウンメニューからアップロードされたイメージを選択し、「次へ」をクリックします。オプションで、ドメイン名フィールドにインスタンスのドメイン名を入力します。
注：名前にスペースを含めることはできません。
 - ネットワーク設定で、管理インターフェイスドロップダウンメニューから、インスタンスを管理するインターフェイスを選択し、そのインターフェイスのIPアドレスとゲートウェイを設定します。高可用性とサービスのためにインターフェイスを明示的に割り当てることができます。パラメータを選択し、「次へ」をクリックします。

注：管理、高可用性、およびサービスのためにインターフェイスを割り当てる際は、サポートされているインターフェイスの組み合わせに基づいてインターフェイスを割り当ててください。

3つすべてに同じインターフェイスを選択できます。3つすべてに異なるインターフェイスを選択できます。管理とサービスに同じインターフェイスを選択し、高可用性には別のインターフェイスを選択できます。「完了」をクリックし、次に「閉じる」をクリックします。インスタンスが作成され、起動し、選択したIPアドレスで構成されます。

インスタンスをプロビジョニングした後、SSH経由でインスタンスにログインして構成を完了します。BlueCat DNS/DHCPサーバーの構成、またはBlueCat Address Managerの制御下に置く方法の詳細については、[<https://care.bluecatnetworks.com>](https://care.bluecatnetworks.com) で入手できるBlueCatドキュメントを参照してください。

BlueCat DNS/DHCPサーバーインスタンスの設定を変更するには、**BlueCat DNS/DHCPインスタンス** ペインから、変更するインスタンスを選択し、「**変更**」をクリックします。BlueCat DNS/DHCP変更ウィザードで、パラメータ設定を変更します。

注：インターフェイスパラメータまたはインスタンスの名前を変更すると、変更を有効にするためにインスタンスが停止して再起動します。

BlueCat DNS/DHCPインスタンスの監視

SDXアプライアンスは、BlueCat DNS/DHCPインスタンスの、インスタンスで実行されている **SDXTools** のバージョンなどの統計情報を収集します。

BlueCat DNS/DHCPインスタンスに関連する統計情報を表示するには：

1. BlueCat DNS/DHCP > インスタンス に移動します。
2. 詳細ペインで、インスタンス名の横にある矢印をクリックします。

BlueCat DNS/DHCP インスタンスの管理

Management Service から、BlueCat DNS/DHCP インスタンスを開始、停止、再起動、強制停止、または強制再起動できます。

Configuration タブで、**BlueCat DNS/DHCP** を展開します。

BlueCat DNS/DHCP インスタンスを開始、停止、再起動、強制停止、または強制再起動するには：

1. インスタンスをクリックします。
2. 詳細ペインで、操作を実行するインスタンスを選択し、次のいずれかのオプションを選択します。
 - 開始
 - シャットダウン
 - 再起動
 - 強制シャットダウン
 - 強制再起動

3. 確認メッセージボックスで、「はい」をクリックします。

BlueCat DNS/DHCP インスタンスの **SDXTools** ファイルをアップグレードする

サードパーティインスタンスで実行されているデーモンである **SDXTools** は、Management Serviceとサードパーティインスタンス間の通信に使用されます。

SDXTools のアップグレードには、ファイルをSDXアプライアンスにアップロードする作業が含まれ、その後、インスタンスを選択してから **SDXTools** をアップグレードします。クライアントコンピューターからSDXアプライアンスに **SDXTools** ファイルをアップロードできます。

SDXTools ファイルをアップロードするには：

1. ナビゲーションペインで、**Management Service**を展開し、**SDXTools Files**をクリックします。
2. 詳細ペインで、**Action**リストから**Upload**を選択します。
3. **SDXTools**ファイルのアップロードダイアログボックスで、**参照**をクリックし、ファイルが含まれているフォルダーに移動して、ファイルをダブルクリックします。
4. **アップロード**をクリックします。

SDXToolsをアップグレードするには：

Configurationタブで、**BlueCat DNS/DHCP**を展開します。

1. **Instances**をクリックします。
2. 詳細ペインで、インスタンスを選択します。
3. Actionリストから、**Upgrade SDXTools**を選択します。
4. **SDXTools**のアップグレードダイアログボックスで、ファイルを選択し、**OK**をクリックしてから、**閉じる**をクリックします。

BlueCat DNS/DHCPインスタンスを再検出する

インスタンスの最新の状態と構成を表示するために、インスタンスを再検出できます。再検出中に、Management Serviceは構成を取得します。デフォルトでは、Management Serviceはすべてのインスタンスの再検出を30分ごとに1回スケジュールします。

「**Configuration**」タブで、「**BlueCat DNS/DHCP**」を展開します。

1. 「**Instances**」をクリックします。

2. 詳細ペインで、再検出するインスタンスを選択し、「**Action**」リストから「**Rediscover**」をクリックします。
3. 「**Confirm**」メッセージボックスで、「**Yes**」をクリックします。

CA アクセス ゲートウェイ

注記:

バージョン14.1ビルド17.x以降、NetScaler SDXはサードパーティ製仮想マシンのサポートを終了しました。

CA Access Gatewayは、スケーラブルで管理しやすく、拡張可能なスタンドアロンサーバーであり、アクセス制御のためのプロキシベースのソリューションを提供します。CA Access Gatewayは、エンタープライズ向けのネットワークゲートウェイを提供し、従来のCookieベースのテクノロジーに依存しない複数のセッションスキームをサポートするプロキシエンジンを採用しています。

組み込みのWebエージェントにより、エンタープライズ全体でシングルサインオン (SSO) が可能になります。CA Access Gatewayは、HTTPおよびHTTPSリクエストのアクセス制御と、CookieレスSSOを提供します。また、この製品はセッション情報をインメモリセッションストアに保存します。プロキシルールは、CA Access Gatewayがエンタープライズ内の宛先サーバーにあるリソースへのリクエストを転送またはリダイレクトする方法を定義します。

ネットワークリソースに単一のゲートウェイを提供することで、CA Access Gatewayは企業ネットワークを分離し、アクセス制御を一元化します。

注: チャンネルの一部であるSR-IOVインターフェイス (1/xおよび10/x) は、CA Access Gatewayインスタンスではチャンネルがサポートされていないため、インターフェイスのリストに表示されません。CA Access Gatewayの機能の詳細については、その製品のドキュメントを参照してください。

CA Access Gatewayインスタンスをプロビジョニングする

CA Access Gatewayインスタンスをプロビジョニングする前に、XVAイメージをダウンロードする必要があります。XVAイメージをダウンロードしたら、SDXアプライアンスにアップロードします。SDXアプライアンスでManagement Serviceバージョン10.5ビルド52.3.e以降を使用していることを確認してください。CA Access Gatewayをプロビジョニングするには、まずXVAイメージ

をSDXアプライアンスにアップロードし、次にインスタンスをプロビジョニングする必要があります。

XVAイメージをSDXアプライアンスにアップロードするには:

1. **Configuration**タブで、**CA Access Gateway > Software Images**の順に移動します。
2. 詳細ペインの**XVA Files**の下にある**Action**ドロップダウンリストから、**Upload**をクリックします。
3. 表示されるダイアログボックスで、**Browse**をクリックし、アップロードするXVAファイルを選択します。
4. **Upload**をクリックします。XVAファイルが**XVA Files**ペインに表示されます。

CA Access Gatewayインスタンスをプロビジョニングするには:

1. **Configuration**タブで、**CA Access Gateway > Instances**に移動します。
2. 詳細ペインで、**追加**をクリックします。
3. Provision CA Access Gatewayウィザードで、画面の指示に従います。
4. **完了**をクリックし、次に**閉じる**をクリックします。

インスタンスをプロビジョニングした後、インスタンスにログオンし、詳細な構成を実行します。

プロビジョニングされたインスタンスのパラメータの値を変更するには、詳細ペインで変更するインスタンスを選択し、**変更**をクリックします。Modify CA Access Gatewayウィザードで、環境に適した値にパラメータを設定します。

注:

インターフェイスパラメータまたはインスタンスの名前を変更すると、変更を有効にするためにインスタンスが停止して再起動します。

CA Access Gatewayインスタンスを監視する

SDXアプライアンスは、インスタンスで実行されている **SDXTools** のバージョンなど、CA Access Gatewayインスタンスの統計情報を収集します。

CA Access Gatewayインスタンスに関連する統計を表示するには:

1. **CA Access Gateway > インスタンス**に移動します。
2. 詳細ペインで、インスタンス名の横にある矢印をクリックします。

CA Access Gatewayインスタンスを管理する

Management ServiceからCA Access Gatewayインスタンスを開始、停止、再起動、強制停止、または強制再起動できます。これらのタスクを完了するには、次の手順に従います。

1. 「**Configuration**」タブで、「**CA Access Gateway**」を展開します。
2. 「**CA Access Gateway > Instances**」に移動します。
3. 詳細ペインで、操作を実行するインスタンスを選択し、次のいずれかのオプションを選択します。
 - 起動
 - シャットダウン
 - 再起動
 - 強制シャットダウン
 - 強制再起動
4. 確認メッセージボックスで、「はい」をクリックします。

パロアルトネットワークス VMシリーズ

注：

バージョン14.1ビルド17.x以降、NetScaler SDXはサードパーティ製仮想マシンのサポートを終了しました。

Palo Alto Networks VM-Series仮想ファイアウォールは、同社の物理セキュリティアプライアンスで利用可能なPAN-OSの機能セットと同じものを使用し、すべての主要なネットワークセキュリティ機能を提供します。NetScaler SDX上のVM-Seriesは、高度なセキュリティ機能とADC機能を単一プラットフォームに統合し、企業、事業部門、サービスプロバイダーの顧客がアプリケーションに安全かつ確実にアクセスできるようにします。NetScaler SDX上のVM-Seriesの組み合わせは、Citrix Virtual Apps and Desktopsの展開向けに、完全で検証済みのセキュリティおよびADCソリューションも提供します。

Management Serviceからインスタンスのプロビジョニング、監視、管理、トラブルシューティングを行うことができます。

注意点：

- SDXアプライアンスにプロビジョニングできるインスタンスの総数は、利用可能なSDXハードウェアリソースに依存します。
- チャンネルの一部であるSR-IOVインターフェイス (1/xおよび10/x) は、Palo Alto VM-Seriesインスタンスではチャンネルがサポートされていないため、インターフェイスのリストに表示されません。Palo Alto Network VM-Seriesの詳細については、[Palo Alto Network Documentation](#)を参照してください。

PaloAlto VM-Seriesインスタンスをプロビジョニングする

Palo Alto VM-Seriesインスタンスをプロビジョニングする前に、[Palo Alto NetworksのWebサイト](#)からXVAイメージをダウンロードする必要があります。XVAイメージをダウンロードしたら、SDXアプライアンスにアップロードします。

XVAイメージをSDXアプライアンスにアップロードするには：

1. **Configuration**タブで、**PaloAlto VM-Series > Software Images**に移動します。
2. 詳細ペインで、**XVA Files**の下にある**Action**ドロップダウンリストから、**Upload**をクリックします。
3. 表示されるダイアログボックスで、**Browse**をクリックし、アップロードするXVAファイルを選択します。
4. **Upload**をクリックします。XVAファイルが**XVA Files**ペインに表示されます。

Palo Alto VM-Series インスタンスをプロビジョニングするには:

1. 「**Configuration**」タブで、「**PaloAlto VM-Series > Instances**」に移動します。
2. 詳細ペインで、**追加**をクリックします。
3. Provision PaloAlto VM-Series ウィザードで、画面の指示に従います。
4. **完了**をクリックし、次に**閉じる**をクリックします。

インスタンスをプロビジョニングした後、インスタンスにログオンし、詳細な構成を実行します。

プロビジョニングされたインスタンスのパラメータの値を変更するには、詳細ペインで変更するインスタンスを選択し、**変更**をクリックします。Modify PaloAlto VM-Series ウィザードで、環境に適した値にパラメータを設定します。

注: インターフェイスパラメータまたはインスタンスの名前を変更すると、変更を有効にするためにインスタンスが停止して再起動します。

Palo Alto VM-Series インスタンスを監視する

SDXアプライアンスは、Palo Alto VM-Series インスタンスで実行されている **SDXTools** のバージョンなどの統計情報を収集します。

Palo Alto VM-Series インスタンスに関連する統計情報を表示するには:

1. 「**PaloAlto VM-Series > Instances**」に移動します。
2. 詳細ペインで、インスタンス名の横にある矢印をクリックします。

PaloAlto VM-Series インスタンスを管理する

Management ServiceからPaloAlto VM-Series インスタンスを開始、停止、再起動、強制停止、または強制再起動できます。

「**Configuration**」タブで、「**PaloAlto VM-Series**」を展開します。

1. 「**PaloAlto VM-Series > Instances**」に移動します。
2. 詳細ペインで、操作を実行するインスタンスを選択し、次のいずれかのオプションを選択します。
 - 起動
 - シャットダウン
 - 再起動
 - 強制シャットダウン
 - 強制再起動
3. 確認メッセージボックスで、「**Yes**」をクリックします。

PaloAlto VM-Seriesインスタンスのトラブルシューティング

Management ServiceからPaloAlto VM-Seriesインスタンスにpingを実行して、デバイスに到達可能かどうかを確認します。Management Serviceからインスタンスへのパケットのルートをトレースして、インスタンスに到達するために必要なホップ数を特定できます。

インスタンスを再検出して、インスタンスの最新の状態と構成を表示します。再検出中に、Management ServiceはSDXアプライアンスで実行されているPaloAlto VM-Seriesの構成とバージョンを取得します。デフォルトでは、Management Serviceは30分ごとにインスタンスの再検出をスケジュールします。

「**Configuration**」タブで、「**PaloAlto VM-Series**」を展開します。

インスタンスにpingを実行するには：

1. 「**Instances**」をクリックします。
2. 詳細ペインで、pingしたいインスタンスを選択し、**アクション**リストから**Ping**をクリックします。**Ping**メッセージボックスにpingが成功したかが表示されます。

インスタンスのルートをトレースするには：

1. **インスタンス**をクリックします。
2. 詳細ペインで、pingしたいインスタンスを選択し、**アクション**リストから**TraceRoute**をクリックします。**Traceroute**メッセージボックスにインスタンスへのルートが表示されます。

インスタンスを再検出するには：

1. **インスタンス**をクリックします。
2. 詳細ペインで、再検出したいインスタンスを選択し、**アクション**リストから**Rediscover**をクリックします。
3. 確認メッセージボックスで、**はい**をクリックします。

SDXにおける帯域幅メータリング

NetScaler SDXの帯域幅メータリングは、正確で信頼性が高く、使いやすいメータリングスキームを提供し、処理能力を効率的に割り当て、帯域幅の使用量を収益化できます。メータリングスキームは、すべてのユーザーが常に割り当てられた帯域幅を得られるように、さまざまなリソース間で帯域幅を最適に割り当てるために必要です。

帯域幅の割り当ては、次の2つのモードで行うことができます。

- 固定スループットレートの専用帯域幅
- 最小保証スループットと帯域幅バースト機能を備えた専用帯域幅

固定スループットレートの専用帯域幅

この帯域幅割り当て方法では、各VPXインスタンスに専用帯域幅が割り当てられます。インスタンスは設定された制限まで帯域幅を使用できます。専用モードでは、割り当てられる最小帯域幅と最大帯域幅は同じです。ある期間中にVPXインスタンスが割り当てられた帯域幅よりも多くの帯域幅を必要とする場合、専用モードではインスタンスはそのスループットを増やすことができません。VPXインスタンスが重要なリクエストを処理する場合、この問題は欠点となる可能性があります。

また、SDXアプライアンスにいくつかのVPXインスタンスがあり、その一部が割り当てられた帯域幅を利用していない場合、専用モードではその未使用の帯域幅を共有することはできません。これらの課題をすべて克服するには、最小保証レートと帯域幅を動的に増加させる機能を備えた専用帯域幅が役立ちます。

最小保証スループットと帯域幅バースト機能を備えた専用帯域幅

この帯域幅割り当て方法では、VPXには最小保証帯域幅が割り当てられ、事前に設定された制限まで帯域幅を増やす柔軟性があります。VPXが使用できる追加の帯域幅は、バースト容量と呼ばれます。

バースト容量の利点は、余剰容量を持つインスタンスと未使用容量を持つVPXがある場合に発揮されます。これらのVPXインスタンスの余剰容量は、割り当てられた帯域幅を完全に利用し、一時的にさらに多くの帯域幅を必要とする他のVPXインスタンスに割り当てることができます。さまざまなサービスプロバイダーも、専用容量を必要とする顧客にさまざまなアドオンサービスを提

供することに関心を持っています。同時に、帯域幅を過剰にプロビジョニングしたくありません。バースト可能な帯域幅は、顧客が特定の帯域幅を保証され、高需要期間中に帯域幅を増やすオプションがあるようなシナリオで役立ちます。

帯域幅割り当てモードの選択

バースト可能なスループットを選択する前に、動的バーストスループット割り当てを有効にする必要があります。このオプションを有効にするには、次の手順に従います。

1. SDX管理コンソールから、**Configuration > System** に移動します。
2. **System Settings** グループから、**Change System Settings** を選択します。
3. 「動的バーストスループット割り当てを有効にする」チェックボックスをクリックして、動的スループットを有効にします。



VPXをプロビジョニングする際、帯域幅バーストまたは動的スループットを選択できます。

1. **SDX Management Service**で、**構成 > NetScaler > インスタンス > 追加**をクリックします。
2. 「**NetScalerのプロビジョニング**」ページが開きます。「**ライセンス割り当て**」で、「**割り当てモード**」から「**バースト可能**」を選択します。



NetScalerインスタンスのプロビジョニング方法の詳細については、「[NetScalerインスタンスのプロビジョニング](#)」を参照してください。

固定レートのスループットを使用する場合は、「**固定**」を選択します。デフォルトでは、帯域幅割り当てには固定モードが設定されています。すべてのVPXインスタンスが同じモードで動作する必要はありません。各VPXインスタンスは異なるモードで構成できます。

注: SDXを10.5.e以前のバージョンから移行する場合、デフォルトでは、すべてのVPXインスタンスは固定割り当てモードになります。

VPXインスタンスの最大バースト帯域幅の決定

各VPXがバーストを許可される範囲は、アルゴリズムによって計算されます。バースト可能な帯域幅を持つVPXをプロビジョニングする場合、そのような各VPXには優先順位を付与する必要があります。バースト可能な帯域幅の割り当ては、このバースト優先順位に依存します。優先順位はP0からP4まであり、P0が最も高く、P4が最も低くなります。

VPX1とVPX2という2つのVPXがあるケースを考えてみましょう。VPX1とVPX2に割り当てられる最小帯域幅は、それぞれ4 Gbpsと2 Gbpsで、それぞれ2 Gbpsと1 Gbpsのバースト可能な帯域幅を持ちます。次の表にパラメータを示します。

VPX名	パラメータ	値	
VPX1	最小保証帯域幅	4ギガbps	
-	-	最大バースト可能帯域幅	2ギガbps
-	-	優先度	P0
VPX2	最小保証帯域幅	2ギガbps	
-	-	最大バースト可能帯域幅	1ギガbps
-	-	優先度	P1

この場合、合計ライセンス帯域幅が8 Gbpsであると仮定します。両方のVPXインスタンスが最大バースト可能制限までバーストしている場合、つまり次のようになります。

1. VPX1がその最大バースト可能帯域幅、つまり2 Gbpsを使用している場合、合計で $4 + 2 = 6$ Gbpsを使用しています。
2. VPX2がその最大バースト可能帯域幅、つまり1 Gbpsを使用している場合、合計で $2 + 1 = 3$ Gbpsを使用しています。

この場合、使用される最大帯域幅は、8 Gbpsのライセンス容量を超えています。そのため、使用量をライセンス容量内の帯域幅に抑えるには、いずれかのVPXがバースト可能帯域幅を放棄する必要があります。この場合、VPX2はVPX1よりも優先度が低いため、1 Gbpsのバースト可能帯域幅を放棄します。VPX1はVPX2よりも優先度が高いため、バーストを継続します。このようなすべてのシナリオにおいて、最小保証帯域幅は常に尊重されるようにします。

スループットとデータ消費統計の確認

各VPXについて、グラフでスループットとデータ消費統計を確認できます。グラフにアクセスするには、次の手順に従います。

1. SDX管理サービスから、**Configuration > NetScaler > Instances** ページに移動します。
2. VPXインスタンスを選択し、**Action drop** リストをクリックします。

3. リストからスループット統計またはデータ使用量統計を選択します。

グラフでは、データ消費量とスループット統計をさまざまな期間で確認できます。例えば：

- 過去1時間
- 過去1日
- 過去1週間
- 過去1か月、および
- 前月

グラフの下部にあるスライダーを調整して、グラフ内の特定の期間を選択することもできます。グラフの線にマウスを移動すると、特定の時間のデータ消費量またはスループットデータを確認できます。

次の図は、1週間のスループットデータのサンプルグラフを示しています。



NetScalerインスタンスの構成と管理

アプライアンスにNetScalerインスタンスをプロビジョニングしたら、インスタンスを構成および管理する準備が整います。まず、サブネットIP（SNIP）アドレスを作成し、構成を保存します。その後、インスタンスで基本的な管理タスクを実行できます。管理構成を適用する必要があるかどうかを確認してください。

警告: インスタンスのプロビジョニングされたネットワークインターフェイスまたはVLANを変更する場合は、インスタンスで直接変更するのではなく、Management Serviceを使用して変更してください。

NetScalerインスタンスでSNIPアドレスを作成する

SDXアプライアンスにプロビジョニングされた後、NetScalerインスタンスにSNIPアドレスを割り当てることができます。

SNIPは接続管理とサーバー監視に使用されます。NetScaler SDXアプライアンスを最初に構成するときにSNIPを指定することは必須ではありません。Management ServiceからNetScalerインスタンスにSNIPを割り当てることができます。

NetScalerインスタンスにSNIPアドレスを追加するには

1. **Configuration**タブのナビゲーションペインで、**NetScaler**をクリックします。
2. 詳細ペインの**NetScaler Configuration**の下で、**Create IP**をクリックします。
3. **Create NetScaler IP**ダイアログボックスで、次のパラメータの値を指定します。
 - **IP Address:** SNIPアドレスとして割り当てられるIPアドレスを指定します。
 - **Netmask:** SNIPアドレスに関連付けられているサブネットマスクを指定します。
 - **Type:** デフォルト値はSNIPです。
 - **Save Configuration:** NetScalerに構成を保存するには選択します。デフォルト値はfalseです。
 - **Instance IP Address:** NetScalerインスタンスのIPアドレスを指定します。
4. 「作成」をクリックし、「閉じる」をクリックします。

構成を保存する

Management Serviceから NetScalerインスタンスの実行中の構成を保存できます。

NetScalerインスタンスの構成を保存するには

1. 「**構成**」タブのナビゲーションペインで、「**NetScaler**」をクリックします。
2. 詳細ペインの「**NetScaler構成**」で、「**構成の保存**」をクリックします。
3. 「**構成の保存**」ダイアログボックスの「**インスタンスIPアドレス**」で、構成を保存する NetScalerインスタンスのIPアドレスを選択します。
4. 「**OK**」をクリックし、「**閉じる**」をクリックします。

NetScalerインスタンスを管理する

Management Serviceでは、NetScalerインスタンスに対して次の操作を実行できます。これらの操作は、「**構成**」タブの「**NetScalerインスタンス**」ペインから、またはホームページのNetScalerインスタンスガジェットから実行できます。

NetScalerインスタンスの起動: Management Serviceユーザーインターフェイスから任意の NetScalerインスタンスを起動します。Management Service UIがこの要求をManagement Serviceに転送すると、NetScalerインスタンスが起動します。

NetScalerインスタンスのシャットダウン: Management Serviceユーザーインターフェイスから任意のNetScalerインスタンスをシャットダウンします。Management Service UIがこの要求をManagement Serviceに転送すると、NetScalerインスタンスが停止します。

NetScalerインスタンスの再起動: NetScalerインスタンスを再起動します。

NetScalerインスタンスの削除: NetScalerインスタンスを使用しない場合は、Management Serviceを使用してそのインスタンスを削除できます。インスタンスを削除すると、そのインスタンスと関連する詳細が SDXアプライアンスのデータベースから完全に削除されます。

NetScalerインスタンスを起動、停止、削除、または再起動するには

1. ナビゲーションペインの「**Configuration**」タブで、「**NetScaler instances**」をクリックします。
2. 操作を実行するNetScalerインスタンスを選択し、「**Start**」または「**Shut Down**」または「**Delete**」または「**Reboot**」をクリックします。
3. 確認メッセージボックスで、「**Yes**」をクリックします。

NetScalerインスタンスファイルを削除する

アプライアンスから、XVA、ビルド、ドキュメント、SSLキー、SSL証明書などのNetScalerインスタンスファイルを削除できます。

NetScalerインスタンスファイルを削除するには

1. ナビゲーションペインの「**Configuration**」タブで、「**NetScaler Configuration**」を展開し、削除するファイルをクリックします。
2. 詳細ペインでファイル名を選択し、「**Delete**」をクリックします。

管理構成を適用する

VPXインスタンスのプロビジョニング時に、Management Serviceは、いくつかのポリシー、インスタンス管理（admin）プロファイル、およびその他の構成をVPXインスタンス上に作成します。Management Serviceが管理構成の適用に失敗した場合、Management ServiceからVPXインスタンスに構成を明示的にプッシュできます。失敗の理由の1つは、Management ServiceとVPXインスタンスが異なるサブネットワーク上にあり、ルーターがダウンしていることかもしれません。もう1つの理由は、両方が同じサブネット上にあるものの、トラフィックが外部スイッチを通過する必要があり、いずれかのリンクがダウンしていることかもしれません。

NetScalerインスタンスに管理構成を適用するには

1. ナビゲーションペインの「**Configuration**」タブで、「**NetScaler**」をクリックします。
2. 詳細ペインの「**NetScaler Configuration**」の下にある「**Apply Admin Configuration**」をクリックします。
3. 「**Apply Admin Configuration**」ダイアログボックスの「**Instance IP Address**」で、管理構成を適用するVPXインスタンスのIPアドレスを選択します。
4. 「**OK**」をクリックします。

SSL証明書をインストールして管理する

SSL証明書をインストールするプロセスでは、まず証明書ファイルとキーファイルをNetScaler SDXアプライアンスにアップロードします。次に、NetScalerインスタンスにSSL証明書をインストールします。SDXアプライアンスにSSL証明書をインストールまたは更新すると、Management Serviceが再起動します。

証明書ファイルをSDXアプライアンスにアップロードする

すべてのSSLトランザクションにおいて、サーバーは有効な証明書と、対応する秘密鍵および公開鍵のペアを必要とします。NetScalerインスタンスにSSL証明書をインストールする際には、証明書ファイルがSDXアプライアンスに存在している必要があります。SSL証明書ファイルをバックアップとしてローカルコンピューターにダウンロードすることもできます。

SSL証明書ペインで、次の詳細を表示できます。

- **名前**

証明書ファイルの名前。

- **最終変更日時**

証明書ファイルが最後に変更された日付。

- **サイズ**

証明書ファイルのサイズ（バイト単位）。

SSL証明書ファイルをSDXアプライアンスにアップロードするには

1. ナビゲーションペインで、を展開し、をクリックします。
2. ペインで、をクリックします。
3. ダイアログボックスで、をクリックし、アップロードする証明書ファイルを選択します。
4. 「アップロード」をクリックします。証明書ファイルがSSL証明書ペインに表示されます。

SSL証明書ファイルをダウンロードしてバックアップを作成するには

1. SSL証明書ペインで、ダウンロードするファイルを選択し、「ダウンロード」をクリックします。
2. メッセージボックスで、「保存」リストから「名前を付けて保存」を選択します。
3. 「名前を付けて保存」メッセージボックスで、ファイルを保存する場所を参照し、「保存」をクリックします。

SDXアプライアンスへのSSLキーファイルのアップロード

任意のSSLトランザクションでは、サーバーは有効な証明書と、対応する秘密鍵および公開鍵のペアを必要とします。NetScalerインスタンスにSSL証明書をインストールする際には、キーファイルがSDXアプライアンスに存在している必要があります。バックアップとして、SSLキーファイルをローカルコンピューターにダウンロードすることもできます。

SSLキーペインでは、次の詳細を表示できます。

- **名前**

キーファイルの名前。

- **最終変更日時**

キーファイルが最後に変更された日付。

- **サイズ**

キーファイルのサイズ（バイト単位）。

SDXアプライアンスにSSLキーファイルをアップロードするには

1. ナビゲーションペインで、Management Service を展開し、SSL Certificate Files をクリックします。
2. SSL Certificate ペインで、SSL Keys タブの Upload をクリックします。
3. Upload SSL Key File ダイアログボックスで、Browse をクリックし、アップロードするキーファイルを選択します。
4. Upload をクリックしてキーファイルを SDX アプライアンスにアップロードします。キーファイルは SSL Keys ペインに表示されます。

SSL キーファイルをダウンロードしてバックアップを作成するには

1. SSL Certificate ペインで、SSL Keys タブのダウンロードするファイルを選択し、Download をクリックします。
2. メッセージボックスで、Save リストから Save as を選択します。
3. Save As メッセージボックスで、ファイルを保存する場所を参照し、Save をクリックします。

NetScaler インスタンスへの SSL 証明書のインストール

Management Service を使用すると、1 つ以上の NetScaler インスタンスに SSL 証明書をインストールできます。SSL 証明書のインストールを開始する前に、SSL 証明書とキーファイルを SDX アプライアンスにアップロードしたことを確認してください。

NetScaler インスタンスに SSL 証明書をインストールするには

1. ナビゲーションペインで、NetScaler をクリックします。

2. 詳細ペインで、NetScaler Configuration の下にある Install SSL Certificates をクリックします。
3. Install SSL Certificates ダイアログボックスで、次のパラメータの値を指定します。(*) は必須フィールドを示します。
 - 証明書ファイル: 有効な証明書のファイル名を指定します。証明書ファイルは SDX アプライアンスに存在する必要があります。
 - キーファイル: 証明書の作成に使用された秘密鍵のファイル名を指定します。キーファイルはSDXアプライアンスに存在している必要があります。
 - 証明書名: NetScalerに追加する証明書とキーのペアの名前を指定します。最大長: 31
 - 証明書形式: NetScalerでサポートされているSSL証明書の形式を指定します。NetScaler SDXアプライアンスは、SSL証明書にPEMおよびDER形式をサポートしています。
 - パスワード: 秘密鍵の暗号化に使用されたパスフレーズを指定します。このオプションは、暗号化された秘密鍵をロードするために使用できます。最大長: 32。

注: パスワードで保護された秘密鍵は、PEM形式でのみサポートされています。

 - 構成の保存: 構成をNetScalerに保存する必要があるかどうかを指定します。デフォルト値はfalseです。
 - インスタンスIPアドレス: SSL証明書をインストールするNetScalerインスタンスのIPアドレスを指定します。
4. 「OK」をクリックし、次に「閉じる」をクリックします。

NetScalerインスタンスでのSSL証明書の更新

NetScalerインスタンスにインストールされているSSL証明書の証明書ファイル、キーファイル、証明書形式などの一部のパラメーターを更新できます。IPアドレスと証明書名は変更できません。

NetScalerインスタンスでSSL証明書を更新するには

1. ナビゲーションペインでNetScalerを展開し、次に「SSL証明書」をクリックします。
2. SSL証明書ペインで、「更新」をクリックします。
3. 「SSL証明書の変更」ダイアログボックスで、次のパラメーターを設定します。
 - 証明書ファイル: 有効な証明書のファイル名。証明書ファイルはSDXアプライアンスに存在している必要があります。
 - キーファイル: 証明書の作成に使用される秘密鍵のファイル名。キーファイルはSDXアプライアンス上に存在する必要があります。

- 証明書形式: NetScaler SDXアプライアンスでサポートされているSSL証明書の形式。アプライアンスはSSL証明書にPEMおよびDER形式をサポートしています。
- パスワード: 秘密鍵の暗号化に使用されたパスフレーズ。このオプションは、暗号化された秘密鍵をロードするために使用できます。最大長: 32文字。

注: パスワードで保護された秘密鍵はPEM形式でのみサポートされています。

- 構成の保存: 構成をSDXアプライアンスに保存する必要があるかどうかを指定します。デフォルト値はfalseです。
- ドメインチェックなし: 証明書の更新中にドメイン名をチェックしません。

4. OKをクリックし、次に「閉じる」をクリックします。

NetScalerインスタンス上のSSL証明書のポーリング

NetScalerインスタンスにログオンした後、そのインスタンスに直接SSL証明書を追加した場合、Management Serviceはこの新しい証明書を認識しません。このシナリオを回避するには、Management ServiceがすべてのNetScalerインスタンスをポーリングして新しいSSL証明書をチェックするポーリング間隔を指定します。Management Serviceからいつでもポーリングを実行することもできます。たとえば、すべてのNetScalerインスタンスからSSL証明書のリストをすぐに取得したい場合などです。

ポーリング間隔を構成するには

1. ナビゲーションペインでNetScalerを展開し、次に「SSL証明書」をクリックします。
2. SSL証明書ペインで、「ポーリング間隔の構成」をクリックします。
3. 「ポーリング間隔の構成」ダイアログボックスで、次のパラメータを設定します。
 - ポーリング間隔: Management ServiceがNetScalerインスタンスをポーリングするまでの時間。
 - 間隔単位: 時間の単位。指定可能な値: 時間、分。デフォルト: 時間。
4. 「OK」をクリックし、次に「閉じる」をクリックします。

即時ポーリングを実行するには

1. ナビゲーションペインでNetScalerを展開し、次に「SSL証明書」をクリックします。
2. 「SSL証明書」ペインで、「今すぐポーリング」をクリックします。
3. 確認ダイアログボックスで「はい」をクリックします。「SSL証明書」ペインが更新され、新しい証明書があればリストに表示されます。

NetScalerインスタンスでL2モードを許可する

レイヤー2 (L2) モードでは、NetScalerインスタンスは学習ブリッジとして機能し、宛先ではないすべてのパケットを転送します。Citrix CloudBridgeなどの一部の機能では、NetScalerインスタンスでL2モードを有効にする必要があります。L2モードが有効になっている場合、インスタンスは自身のMACアドレス以外のMACアドレスのパケットを受信および転送できます。ただし、NetScaler SDXアプライアンスで実行されているNetScalerインスタンスでL2モードを有効にするには、管理者はまずそのインスタンスでL2モードを許可する必要があります。L2モードを許可する場合は、ブリッジンググループを回避するための予防措置を講じる必要があります。

注意事項:

1. 特定の1/xインターフェイスでは、タグなしパケットは1つのインスタンスでのみ許可する必要があります。同じインターフェイスで有効になっている他のすべてのインスタンスについては、 を選択する必要があります。

注:

Citrix®は、L2モードのインスタンスに割り当てられているすべてのインターフェイスでを選択することを推奨します。を選択した場合、そのインターフェイスでタグなしパケットを受信することはできません。

インスタンスに割り当てられたインターフェイスでを選択した場合、そのインスタンスにログオンし、そのインターフェイスでパケットを受信するように802.1q VLANを構成します。

2. L2モードが許可されているNetScalerインスタンスによって共有される1/xおよび10/xインターフェイスについては、次の条件が満たされていることを確認してください。
 - すべてのインターフェイスでVLANフィルタリングが有効になっていること。
 - 各インターフェイスが異なる802.1q VLAN上にあること。
 - インターフェイスでタグなしパケットを受信できるのは1つのインスタンスのみです。そのインターフェイスが他のインスタンスに割り当てられている場合は、それらのインスタンスに対してそのインターフェイスでを選択する必要があります。
3. L2モードが許可されているインスタンスの1/xインターフェイスでタグなしパケットを許可する場合、他のインスタンスはそのインターフェイスでタグなしパケットを受信できません。この条件は、他のインスタンスでL2モードが許可されているかどうかにかかわらず適用されます。
4. L2モードが無効になっているインスタンスの1/xインターフェイスでタグなしパケットを許可する場合、L2モードが許可されているインスタンスは、そのインターフェイスでタグなしパケットを受信できません。

5. L2モードでプロビジョニングされたinstance1に0/xインターフェイスが割り当てられており、そのインターフェイスがinstance2にも割り当てられている場合、instance2に割り当てられている他のすべてのインターフェイスでを選択します。

注: 両方の管理インターフェイスがL2モードのインスタンスに割り当てられている場合、これらのインターフェイスのうち1つのみを、L2モードが有効になっている別のADCインスタンスに割り当てることができます。つまり、両方の管理インターフェイスを、L2モードが有効になっている複数のNetScalerインスタンスに関連付けることはできません。

インスタンスでL2モードを許可するには

1. Provision ADCウィザードまたはModify ADCウィザードで、「**ネットワーク設定**」ページで「**L2モードを許可**」を選択します。 **注:** インスタンスをプロビジョニングするとき、またはインスタンスの実行中に、インスタンスでL2モードを許可する設定を有効にできます。
2. ウィザードの指示に従います。
3. 「完了」をクリックし、その後「閉じる」をクリックします。

インターフェイスでの仮想MACの設定

NetScalerインスタンスは、高可用性（アクティブ-アクティブまたはアクティブ-スタンバイ）構成のために仮想MAC（VMAC）を使用します。仮想MACアドレス（VMAC）は、高可用性セットアップにおいてプライマリノードとセカンダリノードで共有されるフローティングエンティティです。

高可用性セットアップでは、プライマリノードがMIP、SNIP、VIPアドレスなどのすべてのフローティングIPアドレスを所有します。プライマリノードは、これらのIPアドレスに対するアドレス解決プロトコル（ARP）要求に自身のMACアドレスで応答します。その結果、外部デバイス（例えば、アップストリームルーター）のARPテーブルは、フローティングIPアドレスとプライマリノードのMACアドレスで更新されます。

フェールオーバーが発生すると、セカンダリノードが新しいプライマリノードとして引き継ぎます。その後、Gratuitous ARP（GARP）を使用して、プライマリから取得したフローティングIPアドレスをアドバタイズします。ただし、新しいプライマリがアドバタイズするMACアドレスは、自身のインターフェイスのMACアドレスです。

一部のデバイス（特に一部のルーター）は、NetScaler SDXアプライアンスによって生成されたGARPメッセージを受け入れません。このようなデバイスは、古いプライマリノードによってアドバタイズされた古いIP-MACマッピングを保持するため、結果としてサイトがダウンする可能性があります。

この問題は、HAペアの両方のノードでVMACを構成することで解決できます。これにより、両方のノードが同一のMACアドレスを持つことになります。したがって、フェールオーバーが発生しても、セカンダリノードのMACアドレスは変更されず、外部デバイス上のARPテーブルを更新する必要がありません。

VMACの構成は2段階のプロセスです。

1. SDX管理サービスでVMACを構成します。インターフェースまたはLAチャンネルにVRIDを追加します。 [SDX管理サービスでVMACを構成する](#)。
2. CitrixインスタンスでVMACを構成します。詳細については、 [チャンネルでVMACを構成する](#) グループサポート記事を参照してください。

SDX管理サービスでVMACを構成する

VMACを構成するには、管理サービスからインターフェースまたはLAチャンネルにIPv4またはIPv6 VRIDを追加します。管理サービスは内部的にVMACを生成します。NetScalerインスタンスでアクティブ-アクティブモードを構成する際に、同じVRIDを指定します。このアクティブ-アクティブ構成は、Mellanoxインターフェースではサポートされていません。

以下の点に留意してください。

1. 管理サービスからVRIDを追加し、NetScalerインスタンスで同じVRIDを指定します。
NetScalerインスタンスに直接VRIDを追加すると、インスタンスは宛先MACアドレスとしてVMACアドレスを持つパケットを受信できません。
2. 同じSDXアプライアンスで実行されている異なるインスタンスで同じVRIDを使用することはできません。
3. インスタンスの実行中に、インスタンスに割り当てられたインターフェースのVRIDを追加または削除できます。
4. アクティブ-アクティブ構成では、インスタンスに割り当てられたインターフェースに対して複数のVRIDを指定できます。アクティブ-アクティブ展開は、Mellanoxインターフェースではサポートされていません。
5. 10Gインターフェースでは最大86個のVMACが許可され、1Gインターフェースでは最大16個のVMACが許可されます。これ以上VMACフィルターが利用できない場合は、別のインスタンスのVRIDの数を減らしてください。

NetScaler VPXインスタンスを追加する際にVRIDを追加することも、既存のNetScalerインスタンスを変更してVRIDを追加することもできます。

インターフェースまたはLAチャネルにIPv4またはIPv6 VRIDを追加するには

1. SDXでVPXインスタンスを追加する際に、ネットワーク設定でデータインターフェースを選択します。SDXでVPXインスタンスを追加する方法の詳細については、「[NetScalerインスタンスの追加](#)」を参照してください。
2. インターフェースドロップダウンメニューから、インターフェースまたはLAチャネルを選択します。
3. VMAC設定で、次のいずれかまたは両方の値を設定します。
 - VRID IPv4—VMACを識別するIPv4 VRID。指定可能な値: 1～255。
 - VRID IPv6—VMACを識別するIPv6 VRID。指定可能な値: 1～255。注: 複数のVRIDを区切るにはコンマを使用します。例: 12,24。
4. **追加**をクリックして、VMAC設定をインターフェースに追加します。
5. **完了**をクリックし、次に**閉じる**をクリックします。



インスタンスがすでにプロビジョニングされている場合、IPv4またはIPv6 VRIDを追加するには、次の手順に従います。

1. SDX管理サービスから、**構成 > NetScaler > インスタンス**に移動します。
2. インスタンスを選択し、**編集**をクリックします。
3. 「データインターフェース」の下で、インターフェースを選択し、「**編集**」をクリックします。
4. VMAC設定の下で、VRID値を設定します。「**追加**」をクリックし、その後「**完了**」をクリックします。

SDXアプライアンスのNetScalerインスタンスで管理パーティションを設定するために、パーティションMACアドレスを生成する

NetScaler SDXアプライアンス上のNetScalerインスタンスは、管理パーティションと呼ばれる論理エンティティに分割できます。各パーティションは、個別のNetScalerインスタンスとして構成および使用できます。管理パーティションの詳細については、「[管理パーティション](#)」を参照してください。

共有VLAN構成で管理パーティションを使用するには、各パーティションに仮想MACアドレスが必要です。このような仮想MACアドレスは、パーティションMAC (PMAC) アドレスと呼ばれ、共有VLANで受信したトラフィックを分類するために使用されます。このPMACアドレスは、そのパーティションにバインドされているすべての共有VLANで使用されます。

管理パーティションを使用する前に、Management Serviceユーザーインターフェイスを使用してPMACアドレスを生成および構成します。Management Serviceでは、次の方法でパーティションMACアドレスを生成できます。

- ベースMACアドレスを使用する
- カスタムMACアドレスを指定する
- MACアドレスをランダムに生成する

注 パーティションMACアドレスを生成した後、管理パーティションを構成する前にNetScalerインスタンスを再起動する必要があります。

ベースMACアドレスを使用してパーティションMACアドレスを生成するには：

1. **Configuration**タブの左側のペインで、**NetScaler**を展開し、**Instances**をクリックします。
2. **Instances**ペインで、パーティションMACアドレスを生成するNetScalerインスタンスを選択します。
3. **Action**ドロップダウンリストで、**Partition MACs**をクリックします。
4. **Partition MACs**ペインで、**Generate**をクリックします。
5. **Generate Partition MACs**ダイアログボックスの**Generation Method**セクションで、**Using Base Address**を選択します。
6. **Base MAC Address**フィールドに、ベースMACアドレスを入力します。
7. 「**Increment By**」フィールドに、各後続MACアドレスに対してベースMACアドレスをインクリメントする値を入力します。

たとえば、ベースMACアドレスを00:A1:C9:11:C8:11、インクリメント値を2と指定した場合、次のMACアドレスは00:A1:C9:11:C8:13として生成されます。

8. 「**Count**」フィールドに、生成するパーティションMACアドレスの数を入力します。
9. 「**Generate**」をクリックします。

カスタムMACアドレスを指定してパーティションMACアドレスを生成するには：

1. 「**Configuration**」タブの左ペインで、「**NetScaler**」を展開し、「**Instances**」をクリックします。

2. 「**Instances**」 ペインで、パーティションMACアドレスを生成するNetScalerインスタンスを選択します。
3. 「**Action**」 ドロップダウンリストで、「**Partition MACs**」 をクリックします。
4. 「**Partition MACs**」 ペインで、「**Generate**」 をクリックします。
5. 「**Generate Partition MACs**」 ダイアログボックスの「**Generation Method**」 セクションで、「**User Specified**」 を選択します。
6. 「**MAC Addresses**」 フィールドに、MACアドレスを入力します。
7. 「**+**」 アイコンをクリックし、次のMACアドレスを入力します。繰り返して、さらにカスタムMACアドレスを指定します。
8. 「**Generate**」 をクリックします。

パーティションMACアドレスをランダムに生成するには：

1. 「**Configuration**」 タブの左ペインで、「**NetScaler**」 を展開し、「**Instances**」 をクリックします。
2. 「**Instances**」 ペインで、パーティションMACアドレスを生成するNetScalerインスタンスを選択します。
3. 「**Action**」 ドロップダウンリストで、「**Partition MACs**」 をクリックします。
4. 「**Partition MACs**」 ペインで、「**Generate**」 をクリックします。
5. 「**Generate Partition MACs**」 ダイアログボックスの「**Generation Method**」 セクションで、「**Random**」 を選択します。
6. 「**Count**」 フィールドに、生成するパーティションMACアドレスの数を入力します。
7. 「**Generate**」 をクリックします。

SDXアプライアンスでパーティションMACアドレスを生成したら、生成されたパーティションMACアドレスを使用して、NetScalerインスタンスで管理パーティションを設定します。

VPX インスタンスの変更管理

Management Service から NetScaler VPX インスタンスの構成に対する変更を追跡できます。詳細ペインには、デバイス名と IP アドレス、最終更新日時が表示されます。また、保存された構成と実行中の構成の間に違いがあるかどうか也表示されます。デバイスを選択すると、その実行中の構成、保存された構成、構成変更の履歴、およびアップグレード前後の構成の違いを表示できます。VPX インスタンスの構成をローカルコンピューターにダウンロードできます。デフォルトでは、Management Service はすべてのインスタンスを24時間ごとにポーリングしますが、この間隔は変更できます。既存の構成ファイルからコマンドをコピーして、監査テンプレートを作成できま

す。後でこのテンプレートを使用して、インスタンスの構成の変更を見つけ、必要に応じて是正措置を講じることができます。

VPX インスタンスの変更管理を表示するには

1. **Configuration** タブで、**NetScaler > Change Management** に移動します。
2. **Change Management** ペインで、VPX インスタンスを選択し、**Action** リストから次のいずれかを選択します。
 - **Running Configuration**—選択した VPX インスタンスの実行中の構成を新しいウィンドウに表示します。
 - **Saved Configuration**—選択した VPX インスタンスの保存された構成を新しいウィンドウに表示します。
 - **Saved Vs. Running Diff**—保存された構成、実行中の構成、および修正コマンド（差分）を表示します。
 - **Revision History Diff**—ベース構成ファイルと2番目の構成ファイル間の差分を表示します。
 - **Pre vs. Post Upgrade Diff**—アップグレード前後の構成の差分と、修正コマンド（差分）を表示します。
 - **Template Diff**—保存された構成または実行中の構成とテンプレートの差分を表示します。この差分をバッチファイルとして保存できます。テンプレートからインスタンスに構成を適用するには、このバッチファイルをインスタンスに適用します。
 - **Download**—選択した VPX インスタンスの構成をダウンロードし、ローカルデバイスに保存します。

NetScaler インスタンスの構成の更新をポーリングするには

1. **Configuration** タブで、**NetScaler > Change Management** に移動します。
2. **Change Management** ペインで、**Action** リストから次のいずれかを選択します。
 - **今すぐポーリング** — 管理サービスは、アプライアンスにインストールされているVPXインスタンスのいずれかの構成 (ns.conf) の更新を即座にポーリングします。
 - **ポーリング間隔の構成** — 管理サービスがアプライアンスにインストールされているVPXインスタンスのいずれかの構成 (ns.conf) の更新をポーリングするまでの時間。デフォルトのポーリング間隔は24時間です。

NetScalerインスタンスの監査テンプレートを構成するには

1. 既存の構成ファイルを開き、そのコマンドリストをコピーします。

2. **Configuration**タブで、**NetScaler > 変更管理 > 監査テンプレート**に移動します。
3. 詳細ペインで、**追加**をクリックします。
4. **テンプレートの追加**ダイアログボックスで、テンプレートの名前と説明を追加します。
5. **コマンドテキストボックス**に、構成ファイルからコピーしたコマンドリストを貼り付けます。
6. **作成**をクリックし、その後、**閉じる**をクリックします。

チャネルメンバーインターフェースの自動リカバリ

SDXでホストされているVPXインスタンスでは、継続的なTxスToolの発生という稀な事象により、仮想インターフェースがダウンする可能性があります。影響を受ける仮想インターフェースがチャネルの一部である場合、ピアデバイスへの物理接続はまだ稼働しているため、これによりトラフィックのブラックホールが発生する可能性があります。

注記:

異なる種類のインターフェースがエラー無効状態になった場合、結果は次のとおりです。

- チャネルメンバーインターフェースがエラー無効状態になった場合、トラフィックのブラックホールを引き起こします。
- 通常のインターフェースがエラー無効状態になった場合、軽微なトラフィック損失を引き起こし、トラフィックの送信を停止します。

リリース14.1ビルド25.x以降、エラー無効状態の仮想インターフェースを自動的にリカバリし、インターフェースをUP状態に戻すために、仮想インターフェースに対して自動リカバリオプションがデフォルトで有効になっています。

自動リカバリは、仮想インターフェースが静的LAやLACPなどのチャネルにバインドされている場合にのみ発生します。この機能は、VPXインスタンスでコマンド `set channelparam vfautorecover disable/enable` を使用して構成できます。

HAプライマリVPXの仮想インターフェースがダウンし、影響を受けるチャネルでHA監視が有効になっている場合、同じチャネルのすべてのメンバーインターフェースでもVFリセットが発行され、HAフェイルオーバーがトリガーされます。

VPX VF自動リカバリイベントに対してSNMPトラップが生成されるようにするには、VPXインスタンスでSNMPアラーム `interface-auto-recovery` を有効にする必要があります。

NetScaler SDX™ 上でNetScalerインスタンスのディスク領域を拡張する

NetScalerインスタンスのディスク領域拡張機能を使用すると、NetScaler SDX上のNetScalerインスタンスのセカンダリディスク領域を拡張できます。NetScalerインスタンスを削除して再作成することなく、セカンダリディスク領域を拡張できます。この機能は、NetScalerインスタンスが編集されるたびに有効になりますが、NetScalerインスタンスの作成中は無効になります。

この機能には、次の主な利点があります。

- ディスク領域の制限に遭遇することなく、NetScalerファームウェアのアップグレードを容易にします。
- NetScalerインスタンスのワークロードに基づいて、セカンダリディスク領域の要件を柔軟に管理できます。
- ストレージニーズが増加している顧客に対して、よりスムーズな運用を保証します。

このドキュメントでは、管理者がNetScaler SDX上でNetScalerインスタンスのディスク領域拡張を管理するために必要な詳細情報を提供します。

GUIを使用してNetScaler®インスタンスのディスク領域を拡張する

1. **Configuration > NetScaler > Instances** に移動します。
2. NetScalerインスタンスを選択し、**Edit** をクリックします。
3. **Configure NetScaler** ページで、**Resource Allocation** セクションを見つけます。



4. **Additional Disk Size (GB)** フィールドで、追加するディスク領域の値を指定します。
 - セカンダリディスク領域は、10 GB単位でのみ拡張できます。
 - 拡張の最大制限は200 GBです。
5. 希望するディスクサイズを入力した後、**完了**をクリックして変更を保存します。

NetScalerインスタンスのディスク領域の割り当てと拡張

この機能が無効になっている場合、セカンダリディスク領域の割り当ては、次の表に示すように、NetScalerインスタンスのメモリ構成に基づいて決定されます。

NETSCALERインスタンスのメモリ構成	プライマリディスク領域	セカンダリディスク領域
2 GB RAMでNetScalerインスタンスを作成	20 GB	0 GB
4 GB RAMでNetScalerインスタンスを作成	20 GB	42 GB
10 GB RAMでNetScalerインスタンスを作成	20 GB	82 GB
NetScalerインスタンスのメモリを2 GBから4 GBに変更	20 GB	42 GB
NetScalerインスタンスのメモリを4 GBから10 GBに変更	20 GB	以前に割り当てられた42 GBを削除し、新たに82 GBを割り当てます
NetScalerインスタンスのメモリを10 GBから4 GBに変更	20 GB	以前に割り当てられた82 GBを削除し、新たに42 GBを割り当てます
NetScalerインスタンスのメモリを4 GBから2 GBに変更	20 GB	以前に割り当てられた42 GBを削除し、新たに20 GBを割り当てます

この機能が有効になっている場合、割り当てられたセカンダリディスク領域は、次の表に示すように、10 GB単位で拡張できます。

NETSCALERインスタンスのメモリ構成	プライマリディスク領域	セカンダリディスク容量
2 GB RAMでNetScalerインスタンスを作成	20 GB	0 GB
NetScalerインスタンス（2 GB RAM）を編集し、10 GBの追加セカンダリディスク容量を追加	20 GB	20 GB
NetScalerインスタンス（2 GB RAM）を編集し、10 GB	20 GB	30 GB

NETSCALERインスタンスのメモリ構成	プライマリディスク領域	セカンダリディスク容量
の追加セカンダリディスク容量を追加		
4 GB RAMでNetScalerインスタンスを作成	20 GB	42 GB
NetScalerインスタンス (4 GB RAM) を編集し、10 GB の追加セカンダリディスク容量を追加	20 GB	52 GB
NetScalerインスタンス (2 GB RAM) を編集し、10 GB の追加のセカンダリディスク領域を追加します	20 GB	62 GB
10 GB RAM で NetScaler インスタンスを作成します	20 GB	82 GB
NetScalerインスタンス (10 GB RAM) を編集し、10 GB の追加のセカンダリディスク領域を追加します	20 GB	92 GB
NetScalerインスタンス (10 GB RAM) を編集し、10 GB の追加のセカンダリディスク領域を追加します	20 GB	102 GB

NetScalerインスタンスの監視

アプライアンスと、アプライアンスにプロビジョニングされたVPXインスタンスのパフォーマンスの概要は、Management Serviceユーザーインターフェースの監視ページに表示されます。

NetScalerインスタンスをプロビジョニングおよび構成した後、NetScalerインスタンスを監視するためのさまざまなタスクを実行できます。

VPXインスタンスのプロパティを表示する

Management Serviceユーザーインターフェースには、SDXアプライアンスにプロビジョニングされたすべてのVPXインスタンスのリストと説明が表示されます。**NetScalerインスタンス**ペインを使用して、インスタンス名とIPアドレス、CPUとメモリの使用率、スループット、インスタンスに割り当てられた合計メモリなどの詳細を表示します。

VPXインスタンスのIPアドレスをクリックすると、そのインスタンスの構成ユーティリティ（GUI）が新しいタブまたはブラウザで開きます。

VPXインスタンスのプロパティを表示するには

1. 「Configuration」タブの左ペインで、「NetScaler Configuration」を展開し、「Instances」をクリックします。注：VPXインスタンスのプロパティは、「Home」タブからも表示できます。
2. NetScalerインスタンスペインで、NetScalerインスタンスの次の詳細を表示できます。
 - **名前:** プロビジョニング時にNetScalerインスタンスに割り当てられたホスト名。
 - **VMの状態:** 仮想マシンの状態。
 - **NetScalerの状態:** NetScalerインスタンスの状態。
 - **IPアドレス:** NetScalerインスタンスのIPアドレス。IPアドレスをクリックすると、このインスタンスのGUIが新しいタブまたはブラウザで開きます。
 - **Rx (Mbps):** NetScalerインスタンスで受信されたパケット。
 - **Tx (Mbps):** NetScalerインスタンスによって送信されたパケット。
 - **HTTP Req/s:** NetScalerインスタンスで毎秒受信されたHTTPリクエストの合計数。
 - **CPU使用率 (%) :** NetScalerでのCPU使用率のパーセンテージ。
 - **メモリ使用率 (%) :** NetScalerでのメモリ使用率のパーセンテージ。

3. NetScalerインスタンス名の横にある矢印をクリックすると、そのインスタンスのプロパティを表示できます。また、「すべて展開」をクリックすると、すべてのNetScalerインスタンスのプロパティを表示できます。次のプロパティを表示できます。

- **ネットマスク**： NetScalerインスタンスのネットマスクIPアドレス。
- **ゲートウェイ**： デフォルトゲートウェイのIPアドレス。これは、インスタンスがインストールされているサブネットの外部にトラフィックを転送するルーターです。
- **1秒あたりのパケット数**： 毎秒通過するパケットの総数。
- **NIC**： NetScalerインスタンスで使用されるNICの名前と、各インターフェイスに割り当てられた仮想機能。
- **バージョン**： インスタンスで現在実行されているNetScalerソフトウェアのビルドバージョン、ビルド日付、および時刻。
- **ホスト名**： NetScalerインスタンスのホスト名。
- **合計メモリ (GB)**： NetScalerインスタンスに割り当てられている合計メモリ。
- **スループット (Mbps)**： NetScalerインスタンスの合計スループット。
- **稼働開始**： インスタンスが継続的にUP状態になってからの日付と時刻。
- **SSLチップ**： インスタンスに割り当てられているSSLチップの総数。
- **ピアIPアドレス**： HAセットアップの場合、このNetScalerインスタンスのピアのIPアドレス。
- **ステータス**： NetScalerインスタンスで実行されている操作のステータス。たとえば、インスタンスからのインベントリが完了したかどうかのステータスなど。
- **HAマスター状態**： デバイスの状態。この状態は、インスタンスがスタンドアロンまたはプライマリ設定で構成されているか、高可用性設定の一部であることを示します。高可用性設定では、プライマリモードかセカンダリモードかも表示されます。
- **HA同期ステータス**： HA同期ステータスのモード（有効または無効など）。
- **説明**： NetScalerインスタンスのプロビジョニング時に入力された説明。

注:

認証失敗によりADCインスタンスがサービス停止した場合、以下の条件が満たされるとインスタンスの状態の色がグレーに変わります。

- ADCインスタンスのパスワードがインスタンスCLIを使用して直接変更された場合。

- パスワードがManagement Serviceに保存されているインスタンスの管理者プロファイルパスワードと一致しない場合。
- インスタンスを初めて再起動した後、以前のセッションが失われた場合。

通常、インスタンスがサービス停止すると、インスタンスの状態の色は黄色になります。インスタンスを回復するには、次のいずれかを実行します。

- インスタンスCLIから、インスタンスのパスワードをインスタンスの管理者プロファイルのパスワードと一致するように変更します。その後、Management Serviceからインスタンスを再検出します。
- ADCインスタンスの現在のパスワードと同じパスワードで管理者プロファイルを作成します。その後、新しい管理者プロファイルでADCインスタンスを更新します。

NetScalerインスタンスの実行中および保存済み構成を表示する

Management Serviceを使用すると、NetScalerインスタンスの現在実行中の構成を表示できます。また、NetScalerインスタンスの保存済み構成と、構成が保存された時刻も表示できます。

NetScalerインスタンスの実行中および保存済み構成を表示するには

1. 設定タブの左ペインで、NetScaler Configuration を展開し、Instances をクリックします。
2. NetScaler instances ペインで、実行中または保存済みの構成を表示したい NetScaler インスタンスをクリックします。
3. 実行中の構成を表示するには、Running Configuration をクリックし、保存済みの構成を表示するには、Saved Configuration をクリックします。
4. NetScaler Running Config ウィンドウまたは NetScaler Saved Config ウィンドウで、NetScaler インスタンスの実行中または保存済みの構成を表示できます。

NetScaler インスタンスを Ping する

Management Service から NetScaler インスタンスを Ping して、デバイスに到達可能かどうかを確認できます。

NetScaler インスタンスを Ping するには

1. 設定タブの左ペインで、NetScaler Configuration を展開し、Instances をクリックします。
2. NetScaler instances ペインで、Ping したい NetScaler インスタンスをクリックし、Ping をクリックします。Ping メッセージボックスで、Ping が成功したかどうかを確認できます。

NetScaler インスタンスのルートをトレースする

Management Service から NetScaler インスタンスへのパケットのルートを、インスタンスに到達するために使用されるホップ数を決定することでトレースできます。

NetScaler インスタンスのルートをトレースするには

1. 設定タブの左ペインで、NetScaler Configuration を展開し、Instances をクリックします。
2. NetScaler instances ペインで、トレースしたい NetScaler インスタンスをクリックし、TraceRoute をクリックします。Traceroute メッセージボックスで、NetScaler へのルートを確認できます。

NetScaler インスタンスを再検出する

NetScaler インスタンスの最新の状態と構成を表示する必要がある場合に、NetScaler インスタンスを再検出できます。

再検出中に、Management Service は構成をフェッチします。デフォルトでは、Management Service は 30 分ごとにデバイスの再検出をスケジュールします。

注：

リリース 14.1 ビルド 25.x 以降、複数の NetScaler インスタンスを選択して再検出できます。

NetScaler インスタンスを再検出するには

1. **Configuration** タブの左ペインで、**NetScaler Configuration** を展開し、**Instances** をクリックします。
2. **NetScaler instances** ペインで、再検出する NetScaler インスタンスをクリックし、**Rediscover** をクリックします。
3. 確認メッセージボックスで、**Yes** をクリックします。

ログを使用して操作とイベントを監視する

監査ログとタスクログを使用して、Management Service および NetScaler SDX インスタンスで実行された操作を監視します。イベントログを使用して、Management Service および Citrix Hypervisor で実行されたタスクのすべてのイベントを追跡することもできます。

監査ログを表示する

Management Service を使用して実行されたすべての操作は、アプライアンスデータベースにログ記録されます。監査ログを使用して、Management Service ユーザーが実行した操作、日付と時刻、および各操作の成功または失敗のステータスを表示します。適切な列見出しをクリックすることで、ユーザー、操作、監査時刻、ステータスなどで詳細を並べ替えることもできます。

監査ログペインではページネーションがサポートされています。1ページに表示するレコード数を選択します。デフォルトでは、1ページに25件のレコードが表示されます。

監査ログを表示するには、次の手順に従います。

1. ナビゲーションペインで、[監査ログ](#)を展開し、[監査ログ](#)をクリックします。
2. 監査ログペインで、次の詳細を表示できます。
 - **ユーザー名:** 操作を実行した Management Service ユーザー。
 - **IP アドレス:** 操作が実行されたシステムの IP アドレス。
 - **ポート:** 操作が実行されたときにシステムが稼働していたポート。
 - **リソースタイプ:** xen_vpx_image や login など、操作の実行に使用されたリソースのタイプ。
 - **リソース名:** vpx_image_name やログインに使用されたユーザー名など、操作の実行に使用されたリソースの名前。
 - **監査時刻:** 監査ログが生成された時刻。
 - **操作:** add、delete、log out など、実行されたタスク。
 - **ステータス:** 監査のステータス（成功、失敗など）。
 - **メッセージ:** 操作が失敗した場合の失敗の原因、および操作が成功した場合のタスクのステータス（完了など）を説明するメッセージ。

3. 特定のフィールドでログをソートするには、列のヘッダーをクリックします。

タスクログの表示

タスクログを使用して、NetScalerインスタンスでManagement Serviceによって実行される、インスタンスのアップグレードやSSL証明書のインストールなどのタスクを表示および追跡します。タスクログでは、タスクが進行中か、失敗したか、成功したかを確認できます。

タスクログペインではページネーションがサポートされています。1ページに表示するレコード数を選択します。デフォルトでは、1ページに25件のレコードが表示されます。

タスクログを表示するには、次の手順に従います。

1. ナビゲーションペインで、**タスク**を展開し、**タスクログ**をクリックします。
2. ペインで、次の詳細を表示できます。
 - **名前:** 実行中またはすでに実行されたタスクの名前。
 - **ステータス:** タスクのステータス（進行中、完了、失敗など）。
 - **実行者:** 操作を実行したManagement Serviceユーザー。
 - **開始時刻:** タスクが開始された時刻。
 - **終了時刻:** タスクが終了した時刻。

タスクデバイスログの表示

タスクデバイスログを使用して、各SDXインスタンスで実行されているタスクを表示および追跡します。タスクデバイスログでは、タスクが進行中か、失敗したか、成功したかを確認できます。また、タスクが実行されたインスタンスのIPアドレスも表示されます。

タスクデバイスログを表示するには、次の手順に従います。

1. ナビゲーションペインで、**Diagnostics**を展開し、**Task Log**をクリックします。
2. **Task Log**ペインで、タスクをダブルクリックしてタスクデバイスの詳細を表示します。
3. **Task Device Log**ペインで、特定のフィールドでログをソートするには、列のヘッダーをクリックします。

タスクコマンドログの表示

タスクコマンドログを使用して、NetScalerインスタンスで実行されたタスクの各コマンドのステータスを表示します。タスクコマンドログでは、コマンドが正常に実行されたか、失敗したかを確認できます。また、実行されたコマンドと、コマンドが失敗した理由も表示されます。

タスクコマンドログを表示するには、次の手順に従います。

1. ナビゲーションペインで、**Diagnostics**を展開し、**Task Log**をクリックします。
2. **Task Log**ペインで、タスクをダブルクリックしてタスクデバイスの詳細を表示します。
3. **Task Device Log**ペインで、タスクをダブルクリックしてタスクコマンドの詳細を表示します。
4. **Task Command Log**ペインで、特定のフィールドでログをソートするには、列のヘッダーをクリックします。

イベントの表示

Management Serviceユーザーインターフェイスの**Events**ペインを使用して、Management Serviceで実行されたタスクについてManagement Serviceによって生成されたイベントを監視します。

イベントを表示するには、次の手順に従います。

1. 「**System > Events**」に移動します。
2. 「**Events**」ペインで、以下の詳細を表示できます。
 - **Severity:** イベントの重大度。重大、主要、軽微、クリア、情報などがあります。
 - **Source:** イベントが生成されたIPアドレス。
 - **Date:** イベントが生成された日付。
 - **Category:** イベントのカテゴリ（例: PolicyFailed、DeviceConfigChange）。
 - **Message:** イベントを説明するメッセージ。
3. 特定のフィールドでイベントをソートするには、列のヘッダーをクリックします。

NetScaler SDXアプライアンスのユースケース

ネットワークコンポーネント（ファイアウォールやアプリケーションデリバリーコントローラーなど）の場合、マルチテナンシーのサポートは、歴史的に1つのデバイスを複数の論理パーティションに分割する機能を含んでいました。このアプローチにより、多数の個別のデバイスを必要とせずに、各テナントに対して異なるポリシーセットを実装できます。しかし、従来、達成される分離の度合いという点で厳しく制限されていました。

設計上、SDXアプライアンスは同じ制限を受けません。SDXアーキテクチャでは、各インスタンスは専用のNetScalerカーネル、CPUリソース、メモリリソース、アドレス空間、帯域幅割り当てを持つ個別の仮想マシン (VM) として実行されます。SDXアプライアンス上のネットワークI/Oは、システム全体のパフォーマンスを維持するだけでなく、各テナントのデータプレーンおよび管理プレーンのトラフィックを完全に分離することを可能にします。管理プレーンには0/xインターフェースが含まれます。データプレーンには1/xおよび10/xインターフェースが含まれます。データプレーンは管理プレーンとしても使用できます。

SDXアプライアンスの主なユースケースは、管理分離を維持しながら必要なネットワーク数を削減する統合に関連しています。以下に基本的な統合シナリオを示します。

- 管理サービスとNetScalerインスタンスが同じネットワーク内にある場合の統合。
- 管理サービスとNetScalerインスタンスが異なるネットワークにあり、かつすべてのインスタンスが同じネットワークにある場合の統合。
- セキュリティをまたがる統合。
- 各インスタンスに専用インターフェースを持つ統合。
- 複数のインスタンスによる物理ポートの共有を伴う統合。

管理サービスとNetScalerインスタンスが同じネットワークにある場合の統合

SDXアプライアンスにおける統合の単純なケースは、管理サービスとNetScalerインスタンスを同じネットワークの一部として構成することです。このユースケースは、以下の場合に適用できます。

- アプライアンス管理者とインスタンス管理者が同一である。

- 組織のコンプライアンス要件で、管理サービスと異なるインスタンスのNSIPアドレスに対して個別の管理ネットワークが必要であると指定されていない。

インスタンスは同じネットワークにプロビジョニングできます（管理トラフィック用）。VIPアドレスは異なるネットワーク（データトラフィック用）に構成でき、したがって異なるセキュリティゾーンに構成できます。

以下の例では、管理サービスとNetScalerインスタンスは10.1.1.xネットワークの一部です。インターフェイス0/1と0/2は管理インターフェイス、1/1から1/8は1Gデータインターフェイス、10/1から10/4は10Gデータインターフェイスです。各インスタンスには専用の物理インターフェイスがあります。したがって、インスタンスの数はアプライアンスで利用可能な物理インターフェイスの数に制限されます。デフォルトでは、SDXアプライアンスの各インターフェイスでVLANフィルタリングが有効になっています。VLANの数は、1Gインターフェイスでは32、10Gインターフェイスでは63に制限されています。VLANフィルタリングは各インターフェイスで有効/無効にできます。VLANフィルタリングを無効にすると、各インスタンスのインターフェイスごとに最大4096のVLANを構成できます。この例では、各インスタンスに専用インターフェイスがあるため、VLANフィルタリングは不要です。VLANフィルタリングの詳細については、[SDXアプライアンスの管理と監視のVLANフィルタリングセクション](#)を参照してください。

次の図は、上記のユースケースを示しています。

図1. 管理サービスとインスタンスのNSIPが同じネットワークにあるSDXアプライアンスのネットワークトポロジ



次の表に、上記の例でNetScalerインスタンス1をプロビジョニングするために使用されるパラメーターの名前と値を示します。

パラメーター名	インスタンス1の値
名前	vpx8
IPアドレス	10.1.1.2
ネットマスク	255.255.255.0
ゲートウェイ	10.1.1.1
XVAファイル	NS-VPX-XEN-10.0-51.308.a_nc.xva
機能ライセンス	プラチナ

パラメーター名	インスタンス1の値
管理者プロファイル	ns_nsroot_profile
ユーザー名	vpx8
パスワード	Sdx1
パスワードの確認	Sdx1
Shell/Sftp/Scp アクセス	真
合計メモリ (MB)	2048
#SSL チップ	1
スループット (Mbps)	1000
1秒あたりのパケット数	1000000
CPU	共有
インターフェース	0/1 および 1/1

この例に示すように NetScaler インスタンス 1 をプロビジョニングする

1. タブのナビゲーションペインで、 を展開し、 をクリックします。
2. ペインで、 をクリックします。
3. で、ウィザードの指示に従って、前の表に示されているパラメーター値を指定します。
4. をクリックし、 をクリックします。プロビジョニングした NetScaler インスタンスが ペインに表示されます。

管理サービスとNetScalerインスタンスが異なるネットワークにある場合の統合

特定の状況では、アプライアンス管理者は、他の管理者が個々のインスタンスで管理タスクを実行することを許可する場合があります。これは、個々のインスタンス管理者にそのインスタンスのみへのログイン権限を与えることで安全に実行できます。しかし、セキュリティ上の理由から、アプライアンス管理者は、インスタンスが管理サービスと同じネットワーク上にあることを許可し

たかない場合があります。これはサービスプロバイダー環境でよくあるシナリオであり、仮想化とクラウドアーキテクチャを採用する企業でもますます一般的になっています。

次の例では、管理サービスは10.1.1.xネットワークにあり、NetScalerインスタンスは10.1.2.xネットワークにあります。インターフェイス0/1と0/2は管理インターフェイスであり、1/1から1/8は1Gデータインターフェイスであり、10/1から10/4は10Gデータインターフェイスです。各インスタンスには専用の管理者と専用の物理インターフェイスがあります。したがって、インスタンスの数はアプライアンスで利用可能な物理インターフェイスの数に制限されます。各インスタンスには専用のインターフェイスがあるため、VLANフィルタリングは不要です。オプションで、VLANフィルタリングを無効にして、インスタンスあたり、インターフェイスあたり最大4096のVLANを設定できます。この例では、インスタンスが物理インターフェイスを共有しておらず、タグ付きVLANがないため、NSVLANを設定する必要はありません。NSVLANの詳細については、「NetScalerインスタンスの追加」([/ja-jp/sdx/current-release/provision-netscaler-instances.html#add-a-citrix-adc-instance](https://ja-jp/sdx/current-release/provision-netscaler-instances.html#add-a-citrix-adc-instance))を参照してください。

次の図は、前述のユースケースを示しています。

図1. 管理サービスとインスタンスのNSIPが異なるネットワークにあるSDXアプライアンスのネットワークトポロジ



アプライアンス管理者として、管理サービスとNSIPアドレス間のトラフィックをSDXアプライアンス上に維持できます。または、たとえば、トラフィックを外部ファイアウォールやその他のセキュリティ仲介を介してアプライアンスに戻したい場合は、デバイスからトラフィックを強制的にオフにすることができます。

次の表に、この例でNetScalerインスタンス1をプロビジョニングするために使用されるパラメーターの名前と値を示します。

パラメーター名	インスタンス1の値
名前	vpx1
IPアドレス	10.1.2.2
ネットマスク	255.255.255.0
ゲートウェイ	10.1.2.1
XVAファイル	NS-VPX-XEN-10.0-51.308.a_nc.xva
機能ライセンス	プラチナ

パラメーター名	インスタンス1の値
管理者プロファイル	ns_nsroot_profile
ユーザー名	vpx1
パスワード	Sdx1
パスワードの確認	Sdx1
シェル/SFTP/SCPアクセス	真
合計メモリ (MB)	2048
#SSLチップ	1
スループット (Mbps)	1000
1秒あたりのパケット数	1000000
CPU	共有
インターフェース	0/2および1/1

この例に示すようにNetScalerインスタンス1をプロビジョニングするには

1. 「**Configuration**」 タブで、ナビゲーションペインの「**NetScaler Configuration**」を展開し、「**Instances**」をクリックします。
2. NetScalerインスタンスペインで、「**Add**」をクリックします。
3. 「**Provision NetScaler Wizard**」で、ウィザードの指示に従って、前の表に示されている値にパラメータを設定します。
4. 「**Create**」をクリックし、次に「**Close**」をクリックします。プロビジョニングしたNetScalerインスタンスがNetScalerインスタンスペインに表示されます。

セキュリティゾーン間の統合

SDXアプライアンスは、セキュリティゾーン間の統合によく使用されます。DMZは、攻撃者がDMZにのみアクセスできるため、組織の内部ネットワークにセキュリティの追加レイヤーを追加します。組織の内部ネットワークにはアクセスできません。高いコンプライアンスが求められる環境では、DMZと内部ネットワークの両方にVIPアドレスを持つ単一のNetScalerインスタンスは許

容されません。SDXを使用すると、DMZでVIPアドレスをホストするインスタンスと、内部ネットワークでVIPアドレスをホストする他のインスタンスをプロビジョニングできます。

セキュリティゾーンごとに個別の管理ネットワークが必要になる場合があります。DMZ内のインスタンスのNSIPアドレスは、1つのネットワークに配置できます。内部ネットワークにVIPを持つインスタンスのNSIPアドレスは、別の管理ネットワークに配置できます。また、多くの場合、管理サービスとインスタンス間の通信は、ルーターなどの外部デバイスを介してルーティングする必要がある場合があります。ファイアウォールに送信されるトラフィックを制御し、トラフィックをログに記録するようにファイアウォールポリシーを設定できます。

SDXアプライアンスには2つの管理インターフェイス（0/1および0/2）があり、モデルによっては最大8つの1Gデータポートと8つの10Gデータポートがあります。データポートを管理ポートとして使用することもできます（たとえば、タグ付けが管理インターフェイスで許可されていないため、タグ付きVLANを設定する必要がある場合など）。その場合、管理サービスからのトラフィックはアプライアンスを出てからアプライアンスに戻る必要があります。このトラフィックをルーティングするか、オプションでインスタンスに割り当てられたインターフェイスにNSVLANを指定できます。管理インターフェイスがインスタンスと管理サービス間で共通である場合、両者間のトラフィックをルーティングする必要はありません。ただし、セットアップで明示的に要求される場合は、トラフィックをルーティングできます。

各インスタンスに専用インターフェイスを割り当てた統合

以下の例では、インスタンスは複数のネットワークの一部です。インターフェイス0/1は、内部10.1.1.xネットワークの一部である管理サービスに割り当てられています。NetScalerインスタンス2と3は10.1.200.xネットワーク（VLAN 100）の一部です。NetScalerインスタンス4と5は10.1.3.xネットワーク（VLAN 200）の一部です。

オプションで、すべてのインスタンスにNSVLANを設定できます。

次の図は、上記のユースケースを示しています。

図1. 複数のネットワークにNetScalerインスタンスを持つSDXアプライアンスのネットワークトポロジ



SDXアプライアンスはスイッチに接続されています。アプライアンスのポート1/1が接続されているスイッチポートに、VLAN ID 100と200が設定されていることを確認してください。

次の表は、この例でNetScalerインスタンス5と3をプロビジョニングするために使用されるパラメータの名前と値を示しています。

パラメータ名	インスタンス5の値	インスタンス3の値
名前	vpx5	vpx3
IPアドレス	10.1.3.2	10.1.200.2
ネットマスク	255.255.255.0	255.255.255.240
ゲートウェイ	10.1.3.1	10.1.200.1
XVA ファイル	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva
機能ライセンス	プラチナ	プラチナ
管理者プロファイル	ns_nsroot_profile	ns_nsroot_profile
ユーザー名	vpx5	vpx3
パスワード	Sdx1	ルート
パスワードの確認	Sdx1	ルート
シェル/SFTP/SCPアクセス	真	真
合計メモリ (MB)	2048	2048
#SSLチップ	1	1
スループット (Mbps)	1000	1000
1秒あたりのパケット数	1000000	1000000
CPU	共有	共有
インターフェース	1/1 および 10/4	1/1 および 1/5
NSVLAN	200	100
追加 (インターフェイス)	1/1	1/1
タグ付きインターフェイス	Tagged を選択	Tagged を選択

この例に示すように、NetScaler インスタンス 5 および 3 をプロビジョニングするには

1. **Configuration** タブのナビゲーションペインで、**NetScaler Configuration** を展開し、**Instances** をクリックします。
2. NetScaler インスタンスペインで、**Add** をクリックします。
3. **Provision NetScaler Wizard** で、ウィザードの指示に従って、パラメータを前の表に示されている値に設定します。
4. 「作成」をクリックし、次に「閉じる」をクリックします。プロビジョニングしたNetScaler インスタンスがNetScalerインスタンスペインに表示されます。

複数のインスタンスによる物理ポート共有での統合

必要に応じて、インターフェイスでVLANフィルタリングを有効または無効にできます。たとえば、インスタンスで100を超えるVLANを構成するには、そのインスタンスに専用の物理インターフェイスを割り当て、そのインターフェイスでVLANフィルタリングを無効にします。物理インターフェイスを共有するインスタンスではVLANフィルタリングを有効にして、あるインスタンスが別のインスタンスのトラフィックを見ることができないようにします。

注: VLANフィルタリングはアプライアンスのグローバル設定ではありません。インターフェイスでVLANフィルタリングを有効または無効にすると、その設定はそのインターフェイスに関連付けられているすべてのインスタンスに適用されます。VLANフィルタリングが無効になっている場合、最大4096個のVLANを構成できます。VLANフィルタリングが有効になっている場合、10Gインターフェイスでは最大63個のタグ付きVLAN、1Gインターフェイスでは最大32個のタグ付きVLANを構成できます。

次の例では、インスタンスは複数のネットワークの一部です。

- Interface 1/1は、すべてのインスタンスに管理インターフェイスとして割り当てられています。Interface 0/1は、内部10.1.1.xネットワークの一部であるManagement Serviceに割り当てられています。
- NetScalerインスタンス2と3は10.1.200.xネットワークにあり、インスタンス4、5、6、7は10.1.3.xネットワークにあります。インスタンス2と3はそれぞれ専用の物理インターフェイスを持っています。インスタンス4と7は物理インターフェイス1/7を共有し、インスタンス5と6は物理インターフェイス10/4を共有します。
- Interface 1/7でVLANフィルタリングが有効になっています。インスタンス4のトラフィックはVLAN 4用にタグ付けされ、インスタンス7のトラフィックはVLAN 7用にタグ付けされます。その結果、インスタンス4のトラフィックはインスタンス7には見えません。逆に、インスタンス7のトラフィックはインスタンス4には見えません。Interface 1/7では最大32個のVLANを構成できます。

- Interface 10/4ではVLANフィルタリングが無効になっているため、そのインターフェイスで最大4096個のVLANを構成できます。インスタンス5にはVLAN 500～599を、インスタンス6にはVLAN 600～699を構成します。インスタンス5はVLAN 600～699からのブロードキャストおよびマルチキャストトラフィックを見ることができますが、パケットはソフトウェアレベルで破棄されます。同様に、インスタンス6はVLAN 500～599からのブロードキャストおよびマルチキャストトラフィックを見ることができますが、パケットはソフトウェアレベルで破棄されます。

次の図は、上記のユースケースを示しています。

図1. Management ServiceとNetScalerインスタンスがネットワーク全体に分散されたSDXアプリケーションのネットワークトポロジ



次の表に、この例でNetScalerインスタンス7と4をプロビジョニングするために使用されるパラメータの名前と値を示します。

パラメータ名	インスタンス7の値	インスタンス4の値
名前	vpx7	vpx4
IPアドレス	10.1.3.7	10.1.3.4
ネットマスク	255.255.255.0	255.255.255.240
ゲートウェイ	10.1.3.1	10.1.3.1
XVAファイル	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva
機能ライセンス	プラチナ	プラチナ
管理者プロファイル	ns_nsroot_profile	ns_nsroot_profile
ユーザー名	vpx4	vpx4
パスワード	Sdx1	Sdx1
パスワードの確認	Sdx1	Sdx1
シェル/SFTP/SCPアクセス	真	真
合計メモリ (MB)	2048	2048

パラメータ名	インスタンス7の値	インスタンス4の値
SSLチップ数	1	1
スループット (Mbps)	1000	1000
1秒あたりのパケット数	1000000	1000000
CPU	共有	共有
インターフェース	1/1および1/7	1/1および1/7
NSVLAN	200	200

この例でNetScalerインスタンス7と4をプロビジョニングするには

1. **Configuration**タブのナビゲーションペインで、NetScaler Configurationを展開し、**Instances**をクリックします。
2. NetScalerインスタンスペインで、**Add**をクリックします。
3. Provision NetScalerウィザードで、ウィザードの指示に従って、前の表に示されている値にパラメータを設定します。
4. **Create**をクリックし、次に**Close**をクリックします。プロビジョニングしたNetScalerインスタンスがNetScalerインスタンスペインに表示されます。

NITRO API

NetScaler SDX NITROプロトコルを使用すると、SDXアプライアンスをプログラムで設定および監視できます。

NITROは、Representational State Transfer (REST) インターフェイスを通じてその機能を提供します。したがって、NITROアプリケーションは任意のプログラミング言語で開発できます。また、Java、.NET、またはPythonで開発する必要があるアプリケーションの場合、NITROプロトコルは、個別のソフトウェア開発キットとしてパッケージ化された関連ライブラリとして公開されています。

注: NITROを使用する前に、SDXアプライアンスの基本的な理解が必要です。

NITROプロトコルを使用するには、クライアントアプリケーションは以下を必要とします。

- SDXアプライアンスへのアクセス。
- RESTインターフェイスを使用するには、SDXアプライアンスに対してHTTPまたはHTTPSリクエスト（JSON形式のペイロード）を生成するシステムが必要です。任意のプログラミング言語またはツールを使用できます。
- Javaクライアントの場合、Java Development Kit (JDK) 1.5以降のバージョンが利用可能なシステムが必要です。JDKは <http://www.oracle.com/technetwork/java/javase/downloads/index.html> からダウンロードできます。
- .NETクライアントの場合、.NET Framework 3.5以降のバージョンが利用可能なシステムが必要です。.NET Frameworkは<http://www.microsoft.com/downloads/en/default.aspx>からダウンロードできます。
- Pythonクライアントの場合、Python 2.7以降のバージョンとRequestsライブラリ（`<NITRO_SDK_HOME>/lib`で利用可能）がインストールされているシステムが必要です。

NITROパッケージの取得

NITROパッケージは、SDXアプライアンスの構成ユーティリティのダウンロードページでtarファイルとして入手できます。ファイルをダウンロードし、ローカルシステム上のフォルダに解凍する必要があります。このドキュメントでは、このフォルダを`<NITRO_SDK_HOME>`と呼びます。

そのフォルダには、NITROライブラリが lib サブフォルダにあります。NITRO 機能にアクセスするには、ライブラリをクライアントアプリケーションのクラスパスに追加する必要があります。

\<NITRO_SDK_HOME\> フォルダには、NITRO SDK を理解するのに役立つサンプルとドキュメントも用意されています。

注:

```
<div id="sdx-nitro-obtain-con__li_5716E0FF34204411A267E100E8A92067">
```

The REST package contains only documentation for using the REST interfaces.

```
</div>
```

```
<div id="sdx-nitro-obtain-con__li_A72149DD47854CE9B82A5DA88B705828">
```

For the Python SDK, the library must be installed on the client path. For installation instructions, read the \<NITRO_SDK_HOME\>/README.txt file.

```
</div>
```

.NET SDK

SDX NITRO API は、API のスコープと目的に応じて、システム API と設定 API に分類されます。NITRO 操作のトラブルシューティングも可能です。

システムAPI

NITRO を使用するための最初のステップは、SDX アプライアンスとのセッションを確立し、その後、管理者の資格情報を使用してセッションを認証することです。

アプライアンスのIPアドレスと、アプライアンスに接続するためのプロトコル（HTTPまたはHTTPS）を指定して、nitro_serviceクラスのオブジェクトを作成します。次に、このオブジェクトを使用して、管理者のユーザー名とパスワードを指定してアプライアンスにログオンします。

注記：そのアプライアンスにユーザーアカウントが必要です。実行できる設定操作は、アカウントに割り当てられた管理ロールによって制限されます。

次のサンプルコードは、HTTPSプロトコルを使用してIPアドレス10.102.31.16のSDXアプライアンスに接続します。

```
//Specify the IP address of the appliance and service type

nitro_service nitroservice = new nitro_service ("10.102.31.16", "https");


//Specify the login credentials

nitroservice.login("nsroot", "verysecret");
```

注記：アプライアンスでの今後のすべてのNITRO操作で nitro_service オブジェクトを使用してください。

アプライアンスから切断するには、次のようにlogout()メソッドを呼び出します。

```
nitroservice.logout();
```

設定API

NITROプロトコルは、SDXアプライアンスのリソースを設定するために使用できます。

リソースを設定するためのAPIは、com.citrix.sdx.nitro.resource.config.<resource_type>という形式のパッケージまたは名前空間にグループ化されています。これらの各パッケージまたは名前空間には、リソースを設定するためのAPIを提供する<resource_type>という名前のクラスが含まれています。

たとえば、NetScalerリソースには、com.citrix.sdx.nitro.resource.config.nsパッケージまたは名前空間があります。

リソースクラスは、他の操作を実行するためのAPIを提供します。これらの操作には、リソースの作成、リソースとリソースプロパティの取得、リソースの更新、リソースの削除、およびリソースに対する一括操作の実行が含まれます。

リソースの作成

SDXアプライアンス上にリソース (例: NetScalerインスタンス) を作成するには:

1. 対応するプロパティ名を使用して、リソースの必須プロパティの値を設定します。その結果、リソースに必要な詳細を含むリソースオブジェクトが作成されます。注: これらの値はクライアントにローカルに設定されます。オブジェクトがアップロードされるまで、値はアプライアンスに反映されません。
2. 静的add()メソッドを使用して、リソースオブジェクトをアプライアンスにアップロードします。

次のサンプルコードは、SDXアプライアンス上に「ns_instance」という名前のNetScalerインスタンスを作成します。

```
ns newns = new ns();

//Set the properties of the NetScaler locally

newns.name = "ns_instance";

newns.ip_address = "10.70.136.5";

newns.netmask = "255.255.255.0";

newns.gateway = "10.70.136.1";

newns.image_name = "nsvpx-9.3.45_nc.xva";

newns.profile_name = "ns_nsroot_profile";

newns.vm_memory_total = 2048;

newns.throughput = 1000;

newns.pps = 1000000;
```

```
newns.license = "Standard";

newns.username = "admin";

newns.password = "admin";


int number_of_interfaces = 2;

network_interface[] interface_array = new
network_interface[number_of_interfaces];


//Adding 10/1

interface_array[0] = new network_interface();

interface_array[0].port_name = "10/1";


//Adding 10/2

interface_array[1] = new network_interface();

interface_array[1].port_name = "10/2";


newns.network_interfaces = interface_array;


//Upload the NetScaler instance

ns result = ns.add(nitroservice, newns);
```

リソースの詳細を取得する

SDXアプライアンス上のリソースのプロパティを取得するには、次の手順を実行します。

1. get()メソッドを使用してアプライアンスから構成を取得します。その結果、リソースオブジェクトが作成されます。
2. 対応するプロパティ名を使用して、オブジェクトから必要なプロパティを抽出します。

次のサンプルコードは、すべてのNetScaler®リソースの詳細を取得します。

```
//Retrieve the resource object from the SDX appliance

ns[] returned_ns = ns.get(nitroservice);

//Extract the properties of the resource from the object

Console.WriteLine(returned_ns[i].ip_address);

Console.WriteLine(returned_ns[i].netmask);
```

リソース統計を取得する

SDXアプライアンスは、その機能の使用状況に関する統計を収集します。これらの統計はNITROを使用して取得できます。

次のサンプルコードは、ID 123456aのNetScalerインスタンスの統計を取得します。

```
ns obj = new ns();

obj.id = "123456a";

ns stats = ns.get(nitroservice, obj);

Console.WriteLine("CPU Usage:" + stats.ns_cpu_usage);

Console.WriteLine("Memory Usage:" + stats.ns_memory_usage);

Console.WriteLine("Request rate/sec:" +stats.http_req);
```

リソースを更新する

アプライアンス上の既存のリソースのプロパティを更新するには、次の手順を実行します。

1. idプロパティを更新するリソースのIDに設定します。

2. リソースの必須プロパティの値を、対応するプロパティ名を使用して設定します。結果はリソースオブジェクトになります。注: これらの値はクライアントにローカルで設定されます。オブジェクトがアップロードされるまで、これらの値はアプライアンスに反映されません。
3. `update()` メソッドを使用して、リソースオブジェクトをアプライアンスにアップロードします。

次のサンプルコードは、ID 123456a の NetScaler インスタンスの名前を「ns_instance_new」に更新します。

```
ns update_obj = new ns();

//Set the ID of the NetScaler to be updated

update_obj.id = "123456a";

//Get existing NetScaler details

update_obj = ns.get(nitroservice, update_obj);

//Update the name of the NetScaler to "ns_instance_new" locally

update_obj.name = "ns_instance_new";

//Upload the updated NetScaler details

ns result = ns.update(nitroservice, update_obj);
```

リソースを削除する

既存のリソースを削除するには、削除するリソースのIDを引数として渡し、リソースクラスの静的メソッド `delete()` を呼び出します。

次のサンプルコードは、ID 1 の NetScaler インスタンスを削除します。

```
ns obj = new ns();

obj.id = "123456a";

ns.delete(nitroservice, obj);
```

一括操作

複数のリソースを同時に照会または変更できるため、ネットワークトラフィックを最小限に抑えることができます。たとえば、同じ操作で複数の NetScaler SDX アプライアンスを追加できます。

各リソースクラスには、リソースの追加、更新、削除のためにリソースの配列を受け取るメソッドがあります。一括操作を実行するには、各操作の詳細をローカルで指定し、その詳細を一度にサーバーに送信します。

一括操作内の一部の操作の失敗を考慮するために、NITROでは、次のいずれかの動作を構成できます。

- ****終了。**最初のエラーが発生すると、実行は停止します。エラーの前に実行されたコマンドはコミットされます。
- ****続行。**一部のコマンドが失敗しても、リスト内のすべてのコマンドが実行されます。

注: アプライアンスとの接続を確立する際に、`nitro_service()` メソッドで `onerror` パラメータを設定することにより、必要な動作を構成します。

次のサンプルコードは、1回の操作で2つのADCアプライアンスを追加します。

```
ns[] newns = new ns[2];

//Specify details of first NetScaler

newns[0] = new ns();

newns[0].name = "ns_instance1";

newns[0].ip_address = "10.70.136.5";

newns[0].netmask = "255.255.255.0";
```

```
newns[0].gateway = "10.70.136.1";

...

...

//Specify details of second NetScaler

newns[1] = new ns();

newns[1].name = "ns_instance2";

newns[1].ip_address = "10.70.136.8";

newns[1].netmask = "255.255.255.0";

newns[1].gateway = "10.70.136.1";

...

...

//upload the details of the ADC appliances to the NITRO server

ns[] result = ns.add(nitroservice, newns);
```

例外処理

エラーコードフィールドは、操作のステータスを示します。

- エラーコードが0の場合、操作は成功したことを示します。
- ゼロ以外のエラーコードは、NITROリクエストの処理中にエラーが発生したことを示します。

エラーメッセージフィールドには、簡単な説明と障害の性質が記載されています。

`com.citrix.sdx.nitro.exception.nitro_exception` クラスは、NITRO API の実行におけるすべての例外を捕捉します。例外に関する情報を取得するには、`getErrorCode()` メソッドを使用できます。

エラーコードの詳細については、`<NITRO_SDK_HOME>/doc` フォルダにある API リファレンスを参照してください。

REST Web サービス

REST (Representational State Transfer) は、クライアントとサーバー間のシンプルな HTTP リクエストとレスポンスに基づいたアーキテクチャスタイルです。REST は、サーバー側のオブジェクトの状態を照会または変更するために使用されます。REST では、サーバー側はエンティティのセットとしてモデル化され、各エンティティは一意的 URL によって識別されます。

各リソースには状態もあり、その状態に対して以下の操作を実行できます。

- **作成。** クライアントは、「コンテナ」リソース上に新しいサーバー側リソースを作成できます。コンテナリソースはフォルダ、子リソースはファイルまたはサブフォルダと考えることができます。呼び出し元のクライアントは、作成されるリソースの状態を提供します。状態は、XML または JSON 形式を使用してリクエストで指定できます。クライアントは、新しいオブジェクトを識別する一意の URL を指定することもできます。あるいは、サーバーが作成されたオブジェクトを識別する一意の URL を選択して返すこともできます。作成リクエストに使用される HTTP メソッドは POST です。
- **読み取り。** クライアントは、HTTP GET メソッドでリソースの URL を指定することにより、リソースの状態を取得できます。レスポンスメッセージには、JSON 形式で表現されたリソースの状態が含まれます。
- **更新。** 既存のリソースの状態は、そのオブジェクトを識別する URL と、JSON または XML での新しい状態を、PUT HTTP メソッドを使用して指定することで更新できます。
- **削除。** サーバー上に存在するリソースは、DELETE HTTP メソッドと、削除するリソースを識別する URL を使用して破棄できます。

これら 4 つの CRUD 操作 (作成、読み取り、更新、削除) に加えて、リソースは他の操作やアクションをサポートできます。これらの操作は HTTP POST メソッドを使用し、リクエストボディは JSON 形式で、実行する操作とその操作のパラメータを指定します。

SDX NITRO API は、API のスコープと目的に応じて、システム API と構成 API に分類されます。

システム API

NITRO を使用する最初のステップは、SDX アプライアンスとのセッションを確立し、管理者の資格情報を使用してセッションを認証することです。

ログインオブジェクトにユーザー名とパスワードを指定します。作成されたセッション ID は、セッション内のそれ以降のすべての操作のリクエストヘッダーで指定する必要があります。

注: そのアプライアンスにユーザーアカウントが必要です。実行できる構成は、アカウントに割り当てられた管理者ロールによって制限されます。

IP アドレス 10.102.31.16 の SDX アプライアンスに HTTPS プロトコルを使用して接続するには:

- **URL** `https://10.102.31.16/nitro/v2/config/login/`
- **HTTPメソッド** POST
- **リクエスト**
 - **ヘッダー**

```
Content-Type:application/vnd.com.citrix.sdx.login+json
```

注: 以前のバージョンのNITROでサポートされていた「application/x-www-form-urlencoded」などのコンテンツタイプも使用できます。ペイロードが以前のバージョンで使用されていたものと同じであることを確認してください。このドキュメントで提供されているペイロードは、コンテンツタイプが「application/vnd.com.citrix.sdx.login+json」の形式である場合にのみ適用されます。

- **ペイロード**

```
{
  "login":
  {
    "username":"nsroot",
    "password":"verysecret"
  }
}
```

- **応答ペイロード**

- **ヘッダー**

```
HTTP/1.0 201 Created
```

```
Set-Cookie:
```

```
NITRO_AUTH_TOKEN=##87305E9C51B06C848F0942; path=/nitro/v2
```

注: アプライアンスでの今後のすべてのNITRO操作でセッションIDを使用してください。

注: デフォルトでは、アプライアンスへの接続は30分間操作がないと期限切れになります。タイムアウト期間は、新しいタイムアウト期間（秒単位）を ログインオブジェクトで指定することで変更できます。たとえば、タイムアウト期間を60分に変更する場合、リクエストペイロードは次のようになります。

```
{  
  
  "login":  
  
  {  
  
    "username": "nsroot",  
  
    "password": "verysecret",  
  
    "timeout": 3600  
  
  }  
  
}
```

また、操作のリクエストヘッダーにユーザー名とパスワードを指定することで、単一の操作を実行するためにアプライアンスに接続することもできます。たとえば、NetScalerインスタンスの作成中にアプライアンスに接続するには、次のようになります。

- URL
- HTTPメソッド
- リクエスト
 - ヘッダー

```
X-NITRO-USER:nsroot
```

```
X-NITRO-PASS:verysecret
```

```
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

- ペイロード

```
{  
  
  "ns":  
  
  {  
  
    ...  
  
  }  
  
}
```

- 応答。

- ヘッダー

```
HTTP/1.0 201 Created
```

アプライアンスから切断するには、DELETE メソッドを使用します:

- URL

- HTTP メソッド DELETE

- リクエスト

- ヘッダー

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
```

```
Content-Type:application/vnd.com.citrix.sdx.login+json
```

構成 API

NITRO プロトコルは、SDX アプライアンスのリソースを構成するために使用できます。

各 SDX リソースには、実行される操作の種類に応じて、一意の URL が関連付けられています。

構成操作の URL の形式は次のとおりです: `http://<IP>/nitro/v2/config/<resource_type>`

リソースの作成

SDX アプライアンスでリソース (たとえば、NetScaler インスタンス) を作成するには、特定のリソースオブジェクトでリソース名とその他の関連引数を指定します。たとえば、vpx1 という名前の NetScaler インスタンスを作成するには:

- URL
- HTTP メソッド
- リクエスト
 - ヘッダー

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
```

```
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

- ペイロード

```
{
  "ns":
  {
    "name": "vpx1",
    "ip_address": "192.168.100.2",
    "netmask": "255.255.255.0",
    "gateway": "192.168.100.1",
    "image_name": "nsvpx-9.3-45_nc.xva",
    "vm_memory_total": 2048,
```

```
    "throughput":1000,  
  
    "pps":1000000,  
  
    "license":"Standard",  
  
    "profile_name":"ns_nsroot_profile",  
  
    "username":"admin",  
  
    "password":"admin",  
  
    "network_interfaces":  
  
    [  
  
        {  
  
            "port_name":"10/1"  
  
        },  
  
        {  
  
            "port_name":"10/2"  
  
        }  
  
    ]  
  
}
```

リソースの詳細と統計の取得

SDXリソースの詳細は、次のように取得できます。

- SDXアプライアンス上の特定のリソースの詳細を取得するには、URLでそのリソースのIDを指定します。
- 特定のフィルターに基づいてリソースのプロパティを取得するには、URLでフィルター条件を指定します。

URLの形式は次のとおりです: `http://<IP>/nitro/v2/config/<resource_type>?filter=<property1>:<value>,<property2>:<value>`

- リクエストによってアプライアンスから多数のリソースが返される可能性がある場合は、それらを「ページ」に分割し、ページごとに取得することで、これらの結果をチャンクで取得できます。

たとえば、53個のNetScalerインスタンスを持つSDX上のすべてのNetScalerインスタンスを取得したいとします。53個すべてを1つの大きな応答で取得する代わりに、結果をそれぞれ10個のNetScalerインスタンスのページに分割するように設定し（合計6ページ）、サーバーからページごとに取得します。

ページサイズクエリ文字列パラメータでページ数を指定し、ページ番号クエリ文字列パラメータを使用して取得したいページ番号を指定します。URLの形式は次のとおりです: `http://<IP>/nitro/v2/config/<resource_type>?pageno=<value>&pagesize=<value>`

すべてのページを取得する必要はなく、ページを順番に取得する必要もありません。各リクエストは独立しており、リクエスト間でページサイズの設定を変更することもできます。

注: リクエストによって返される可能性のあるリソースの数を把握するには、リソース自体ではなく、返されるリソースの数を要求するためにcountクエリ文字列パラメータを使用できます。利用可能なNetScalerインスタンスの数を取得する場合、URLは次のようになります。

`http://<IP>/nitro/v2/config/<resource_type>?count=yes`

ID 123456aのNetScalerインスタンスの構成情報を取得するには:

- **URL**
- **HTTPメソッド GET**

リソースを更新する

既存のSDXリソースを更新するには、PUT HTTPメソッドを使用します。HTTPリクエストペイロードで、変更する必要がある名前とその他の引数を指定します。たとえば、ID 123456aのNetScalerインスタンスの名前をvpx2に変更するには、次のようになります。

- **URL**
- **HTTPメソッド**
- **リクエストペイロード**
 - **ヘッダー**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
```

```
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

。ペイロード

```
{  
  
  "ns":  
  
  {  
  
    "name": "vpx2",  
  
    "id": "123456a"  
  
  }  
  
}
```

リソースを削除する

既存のリソースを削除するには、URLで削除するリソースの名前を指定します。たとえば、ID 123456aのNetScalerインスタンスを削除するには、次のようになります。

- URL
- HTTPメソッド
- リクエスト

。ヘッダー

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
```

```
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

一括操作

複数のリソースを同時に照会または変更できるため、ネットワークトラフィックを最小限に抑えることができます。たとえば、同じ操作で複数のNetScaler SDXアプライアンスを追加できます。また、1つのリクエストで異なるタイプのリソースを追加することもできます。

バルク操作内の一部の操作の失敗を考慮して、NITROでは以下のいずれかの動作を構成できます。

- **終了。** 最初のエラーが発生すると、実行は停止します。エラーの前に実行されたコマンドはコミットされます。
- **続行。** 一部のコマンドが失敗した場合でも、リスト内のすべてのコマンドが実行されます。

注: 必要な動作は、リクエストヘッダーで `X-NITRO-ONERROR` パラメーターを使用して構成します。

1つの操作で2つのNetScalerリソースを追加し、いずれかのコマンドが失敗した場合でも続行するには：

- **URL。**
- **HTTPメソッド。**
- **リクエストペイロード。**

◦ **ヘッダー**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue

Content-Type:application/vnd.com.citrix.sdx.ns+json

X-NITRO-ONERROR:continue
```

◦ **ペイロード**

```
{

  "ns":

  [

    {

      "name":"ns_instance1",

      "ip_address":"10.70.136.5",

      "netmask":"255.255.255.0",
```

```

        "gateway": "10.70.136.1"
    },
    {
        "name": "ns_instance2",
        "ip_address": "10.70.136.8",
        "netmask": "255.255.255.0",
        "gateway": "10.70.136.1"
    }
]
}

```

1つの操作で複数のリソース（NetScalerと2人のMPSユーザー）を追加し、いずれかのコマンドが失敗した場合でも続行するには：

- URL。
- HTTPメソッド。 POST
- リクエストペイロード。
 - ヘッダー

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
```

```
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

```
X-NITRO-ONERROR:continue
```

- ペイロード

```

{
    "ns":

```

```
[  
  
  {  
  
    "name": "ns_instance1",  
  
    "ip_address": "10.70.136.5",  
  
    "netmask": "255.255.255.0",  
  
    "gateway": "10.70.136.1"  
  
  },  
  
  {  
  
    "name": "ns_instance2",  
  
    "ip_address": "10.70.136.8",  
  
    "netmask": "255.255.255.0",  
  
    "gateway": "10.70.136.1"  
  
  }  
  
],  
  
"mpsuser":  
  
[  
  
  {  
  
    "name": "admin",  
  
    "password": "admin",  
  
    "permission": "superuser"  
  
  },  
  
  {
```

```
        "name": "admin",

        "password": "admin",

        "permission": "superuser"

    }

]

}
```

例外処理

エラーコードフィールドは、操作のステータスを示します。

- エラーコードが0の場合、操作は成功したことを示します。
- ゼロ以外のエラーコードは、NITROリクエストの処理におけるエラーを示します。

エラーメッセージフィールドは、簡単な説明と障害の性質を提供します。

NITROの仕組み

NITROインフラストラクチャは、クライアントアプリケーションと、NetScaler SDXアプライアンス上で動作するNITRO Webサービスで構成されています。クライアントアプリケーションとNITRO Webサービス間の通信は、HTTPまたはHTTPSを使用するRESTアーキテクチャに基づいています。

図1. NITROのワークフロー



ワークフローの詳細な手順:

1. クライアントアプリケーションは、RESTリクエストメッセージをNITRO Webサービスに送信します。SDKを使用する場合、API呼び出しは適切なRESTリクエストメッセージに変換されます。
2. WebサービスはRESTリクエストメッセージを処理します。
3. NITRO Webサービスは、対応するRESTレスポンスメッセージをクライアントアプリケーションに返します。SDKを使用する場合、RESTレスポンスメッセージはAPI呼び出しに対する適切なレスポンスに変換されます。

ネットワーク上のトラフィックを最小限に抑えるため、サーバーからリソースの完全な状態を取得します。リソースの状態をローカルで変更します。その後、1回のネットワークトランザクションでサーバーにアップロードし直します。

注: リソースに対するローカル操作（そのプロパティの変更）は、オブジェクトの状態が明示的にアップロードされるまで、サーバー上の状態には影響しません。

NITRO APIは本質的に同期型です。つまり、クライアントアプリケーションは、別のNITRO APIを実行する前に、NITRO Webサービスからの応答を待ちます。

ジャバ SDK

SDX NITRO APIは、APIの範囲と目的に応じて、システムAPIと構成APIに分類されます。NITRO操作のトラブルシューティングも可能です。

システムAPI

NITROを使用するための最初のステップは、SDXアプライアンスとのセッションを確立し、管理者の資格情報を使用してセッションを認証することです。

アプライアンスのIPアドレスと、アプライアンスに接続するためのプロトコル（HTTPまたはHTTPS）を指定して、`nitro_service`クラスのオブジェクトを作成します。次に、このオブジェクトを使用して、管理者のユーザー名とパスワードを指定してアプライアンスにログオンします。

注: そのアプライアンスにユーザーアカウントが必要です。実行できる構成操作は、アカウントに割り当てられた管理ロールによって制限されます。

次のサンプルコードは、HTTPSプロトコルを使用してIPアドレス10.102.31.16のSDXアプライアンスに接続します。

```
//Specify the IP address of the appliance and service type

nitro_service nitroservice = new nitro_service ("10.102.31.16", "https");

//Specify the login credentials

nitroservice.login("nsroot", "verysecret");
```

注: アプライアンスでの今後のすべてのNITRO操作で、`nitro_service`オブジェクトを使用してください。

アプライアンスから切断するには、次のように `logout()` メソッドを呼び出します。

```
nitroservice.logout();
```

構成API

NITROプロトコルは、SDXアプライアンスのリソースを構成するために使用できます。

リソースを構成するためのAPIは、`com.citrix.sdx.nitro.resource.config.<resource_type>`という形式のパッケージまたは名前空間にグループ化されています。これらの各パッケージまたは名前空間には、リソースを構成するためのAPIを提供する<resource_type>という名前のクラスが含まれています。

たとえば、NetScalerリソースには、`com.citrix.sdx.nitro.resource.config.ns`パッケージまたは名前空間があります。

リソースクラスは、他の多くの操作を実行するためのAPIを提供します。これらの操作には、リソースの作成、リソースの詳細と統計の取得、リソースの更新、リソースの削除、およびリソースに対する一括操作の実行が含まれます。

リソースの作成

SDXアプライアンス上にリソース（例：NetScalerインスタンス）を作成するには、次の手順を実行します。

1. 対応するプロパティ名を使用して、リソースの必須プロパティの値を設定します。結果として、リソースに必要な詳細を含むリソースオブジェクトが作成されます。注：これらの値はクライアント上でローカルに設定されます。オブジェクトがアップロードされるまで、これらの値はアプライアンスに反映されません。
2. 静的 `add()` メソッドを使用して、リソースオブジェクトをアプライアンスにアップロードします。

次のサンプルコードは、SDXアプライアンス上に「`ns_instance`」という名前のNetScalerインスタンスを作成します。

```
ns newns = new ns();

//Set the properties of the NetScaler locally
```

```
newns.set_name("ns_instance");

newns.set_ip_address("10.70.136.5");

newns.set_netmask("255.255.255.0");

newns.set_gateway("10.70.136.1");

newns.set_image_name("nsvpx-9.3.45_nc.xva");

newns.set_profile_name("ns_nsroot_profile");

newns.set_vm_memory_total(new Double(2048));

newns.set_throughput(new Double(1000));

newns.set_pps(new Double(1000000));

newns.set_license("Standard");

newns.set_username("admin");

newns.set_password("admin");


int number_of_interfaces = 2;

network_interface[] interface_array = new
network_interface[number_of_interfaces];


//Adding 10/1

interface_array[0] = new network_interface();

interface_array[0].set_port_name("10/1");


//Adding 10/2
```

```
interface_array[1] = new network_interface();

interface_array[1].set_port_name("10/2");

newns.set_network_interfaces(interface_array);

//Upload the NetScaler instance

ns result = ns.add(nitroservice, newns);
```

リソースの詳細の取得

SDXアプライアンス上のリソースのプロパティを取得するには、次の手順を実行します。

1. get() メソッドを使用して、アプライアンスから構成を取得します。結果はリソースオブジェクトです。
2. 対応するプロパティ名を使用して、オブジェクトから必要なプロパティを抽出します。

次のサンプルコードは、すべてのNetScaler®リソースの詳細を取得します。

```
//Retrieve the resource object from the SDX appliance

ns[] returned_ns = ns.get(nitroservice);

//Extract the properties of the resource from the object

System.out.println(returned_ns[i].get_ip_address());

System.out.println(returned_ns[i].get_netmask());
```

リソース統計の取得

SDXアプライアンスは、その機能の使用状況に関する統計を収集します。これらの統計はNITROを使用して取得できます。

次のサンプルコードは、ID 123456a のNetScalerインスタンスの統計を取得します。

```
ns obj = new ns();

obj.set_id("123456a");

ns stats = ns.get(nitroservice, obj);

System.out.println("CPU Usage:" + stats.get_ns_cpu_usage());

System.out.println("Memory Usage:" + stats.get_ns_memory_usage());

System.out.println("Request rate/sec:" +stats.get_http_req());
```

リソースの更新

アプライアンス上の既存のリソースのプロパティを更新するには、次の手順を実行します。

1. id プロパティを、更新するリソースのIDに設定します。
2. リソースの必須プロパティの値を、対応するプロパティ名を使用して設定します。結果はリソースオブジェクトになります。注: これらの値はクライアント上でローカルに設定されます。オブジェクトがアップロードされるまで、これらの値はアプライアンスに反映されません。
3. update() メソッドを使用して、リソースオブジェクトをアプライアンスにアップロードします。

次のサンプルコードは、ID 123456a の NetScaler インスタンスの名前を「ns_instance_new」に更新します。

```
ns update_obj = new ns();

//Set the ID of the NetScaler to be updated

update_obj.set_id("123456a");

//Get existing NetScaler details

update_obj = ns.get(nitroservice, update_obj);
```

```
//Update the name of the NetScaler to "ns_instance_new" locally  
  
update_obj.set_name("ns_instance_new");  
  
//Upload the updated NetScaler details  
  
ns result = ns.update(nitroservice, update_obj);
```

リソースの削除

既存のリソースを削除するには、削除するリソースのIDを引数として渡し、リソースクラスの静的メソッド `delete()` を呼び出します。

次のサンプルコードは、ID 1 の NetScaler インスタンスを削除します。

```
ns obj = new ns();  
  
obj.set_id("123456a");  
  
ns.delete(nitroservice, obj);
```

一括操作

複数のリソースを同時に照会または変更できるため、ネットワークトラフィックを最小限に抑えることができます。たとえば、同じ操作で複数のNetScaler SDXアプライアンスを追加できます。

各リソースクラスには、リソースの追加、更新、削除のためにリソースの配列を受け取るメソッドがあります。一括操作を実行するには、各操作の詳細をローカルで指定し、その詳細を一度にサーバーに送信します。

一括操作内の一部の操作の失敗を考慮して、NITROでは次のいずれかの動作を構成できます。

- **終了。** 最初のエラーが発生すると、実行は停止します。エラーの前に実行されたコマンドはコミットされます。
- **続行。** 一部のコマンドが失敗した場合でも、リスト内のすべてのコマンドが実行されます。

注: アプライアンスとの接続を確立する際に、 `onerror` パラメータを `nitro_service()` メソッドで設定して、必要な動作を構成します。

次のサンプルコードは、1回の操作で2つのADCアプライアンスを追加します。

```
ns[] newns = new ns[2];

//Specify details of first NetScaler

newns[0] = new ns();

newns[0].set_name("ns_instance1");

newns[0].set_ip_address("10.70.136.5");

newns[0].set_netmask("255.255.255.0");

newns[0].set_gateway("10.70.136.1");

...

...

...

//Specify details of second NetScaler

newns[1] = new ns();

newns[1].set_name("ns_instance2");

newns[1].set_ip_address("10.70.136.8");

newns[1].set_netmask("255.255.255.0");

newns[1].set_gateway("10.70.136.1");

...

...
```

```
//upload the details of the NetScalers to the NITRO server  
  
ns[] result = ns.add(nitroservice, newns);
```

例外処理

エラーコードフィールドは、操作のステータスを示します。

- エラーコードが0の場合、操作は成功したことを示します。
- ゼロ以外のエラーコードは、NITROリクエストの処理におけるエラーを示します。

エラーメッセージフィールドは、簡潔な説明と障害の性質を提供します。

`com.citrix.sdx.nitro.exception.nitro_exception`クラスは、NITRO APIの実行におけるすべての例外をキャッチします。例外に関する情報を取得するには、`getErrorCode()` メソッドを使用できます。

エラーコードの詳細については、`<NITRO_SDK_HOME>/doc` フォルダーで利用可能なAPIリファレンスを参照してください。

fix

This is the content for the sample heading topic. It is hidden from the main table of contents but remains accessible via links.